P-660R-F1

ADSL2+ Access Router

Support Notes

Version 3.70
May. 2011

All contents copyright © 2011 ZyXEL Communications Corporation.

INDEX

ZyNOS FAQ 4
1. What is ZyNOS? 4
2. How do I access the P-660R-F1 Command Line Interface (CLI)? 4
3. How do I update the firmware and configuration file ? 4
4. How do I upgrade/backup the ZyNOS firmware by using TFTP client program via LAN? 5
5. How do I restore P-660R-F1 configurations by using TFTP client program via LAN? 5
6. What should I do if I forget the system password? 5
7. How to use the Reset button? 5
8. What is SUA? When should I use SUA? 5
9. Is it possible to access a server running behind SUA from the outside Internet? How can I do it? 6
10. How many network users can the SUA/NAT support? 6
11. What are Device filters and Protocol filters? 6
12. How can I protect against IP spoofing attacks? 6

Product FAQ 8
1. How can I manage P-660R-F1? 8
2. What is the default password for Web Configurator? 8
3. How do I know the P-660R-F1's WAN IP address assigned by the ISP? 8
4. What is Traffic Shaping? 8
5. Why do we perform traffic shaping in the P-660R-F1? 8
6. What do the parameters (PCR, SCR, and MBS) mean? 8
7. What do the ATM QoS Types (CBR, UBR, VBR, rtVBR, nrtVBR) mean? 9
8. The P-660R-F1 supports Bridge and Router mode, what's the difference between them? 9
9. How do I know I am using PPPoE? 10
10. Why does my provider use PPPoE? 10
11. When do I need to choose dynamic IP? 10
12. What is DDNS? 12
13. When do I need DDNS service? 12
14. What is DDNS wildcard? Does the P-660R-F1 support DDNS wildcard? 12
15. Can the P-660R-F1's SUA (Simple IP) handle IPSec packets sent by the IPSec gateway? 12
16. What is UPnP? 13

ADSL FAQ 14
1. How does ADSL compare to Cable modems? 14
2. What is the micro-filter or splitter used for? 14
3. How do I know the ADSL line is up? 14
4. How does the P-660R-F1 work on a noisy ADSL? 14
5. Does the VC-based multiplexing perform better than the LLC-based multiplexing? 14
6. How do I know the details of my ADSL line statistics? 15
7. What are the signaling pins of the ADSL connector? 15

Application Notes 16

All contents copyright © 2011 ZyXEL Communications Corporation.

1. Internet Access Using P-660R-F1 under Bridge mode 16
2. Internet Access Using P-660R-F1 under Routing mode 19
3. Setup the P-660R-F1 as a DHCP Relay 22
4. SUA Notes 23
5. Using the Dynamic DNS (DDNS) 32
6. QoS (802.1Q) 34
7. Network Management Using SNMP 40
8. Using system log 42
9. Using IP Alias 44
10. Using IP Policy Routing 46
11. Using Call Scheduling 48
12. Using IP Multicast 50
13. Using Zero-Configuration 51

Support Tool 55
1. Firmware/Configurations Uploading and Downloading using TFTP 55
2. Using FTP to Upload the Firmware and Configuration Files 57

CI Command Reference 58

All contents copyright © 2011 ZyXEL Communications Corporation.

ZyNOS FAQ

1. What is ZyNOS?

ZyNOS is ZyXEL's proprietary Network Operating System. It is the platform on all Prestige routers that delivers network services and applications. It is designed in a modular fashion so it is easy for developers to add new features. New ZyNOS software upgrades can be easily downloaded from our FTP sites as they become available.

2. How do I access the P-660R-F1 Command Line Interface (CLI)?

The Command Line Interface is for the administrator use only, and it could be accessed via telnet session.
Begin telnet session:
(1) Choose “start” on your computer →“run”
(2) Input “cmd” and enter
(3) Input “telnet xxx.xxx.xxx.xxx” (note that there is a space between the two),
(4) Enter to login in the CLI.
Note: It is protected by super password, “1234” by factory default.

3. How do I update the firmware and configuration file?

You can do this if you access the P-660R-F1 as administrator. You can upload the firmware and configuration file to P-660R-F1 from Web Configurator, or using FTP software. You CAN NOT upload the firmware and configuration file via Telnet because the Telnet connection will be dropped during uploading the firmware. Please do not power off the router right after the FTP uploading is finished, the router will upload the firmware to its flash at this moment.

(1) Update on web configuration page, Advanced Setup，
Maintenance -> Tools -> Firmware

You can check your current firmware version and upgrade the firmware of the Router in this page. Make sure the firmware you want to use is on the local hard drive of the computer. Click on Browse to browse the local hard drive and locate the firmware to be used for upgrade.

(2) Update firmware with FTP

a) Use the FTP client program in your PC to login to your P-660R-F1.

Note that it is protected by user name and password, “admin” and “1234” by default.
b) To update firmware, you need to use the command: **put xx.bin ras** for firmware or **put xx.rom rom-0** for rom file.
xx.bin means the firmware on your local hard drive and xx.rom means rom file on your local hard drive. You can simply draw them into the window.

All contents copyright © 2011 ZyXEL Communications Corporation.

Note: There may be firmware that could not be upgraded from Web Configurator. In this case, ZyXEL will prepare special Upload Software

for you. Please read the firmware release note carefully when you want to upload a new firmware.

4. How do I upgrade/backup the ZyNOS firmware by using TFTP client program via LAN?

The P-660R-F1 allows you to transfer the firmware to P-660R-F1 using TFTP program via LAN. The procedure for uploading ZyNOS via TFTP is as follows.

a. Use the TELNET client program in your PC to login to your P-660R-F1.
b. Enter CI command **'sys stdio 0'** to disable Stdio idle timeout
c. To upgrade firmware, use TFTP client program to put firmware in file **'ras'** in the Prestige. After data transfer is finished, the P-660R-F1 will program the upgraded firmware into FLASH ROM and reboot itself.
d. To backup your firmware, use the TFTP client program to get file **'ras'** from the Prestige.

5. How do I restore P-660R-F1 configurations by using TFTP client program via LAN?

a. Use the TELNET client program in your PC to login to your P-660R-F1.
b. Enter CI command **'sys stdio 0'** disable Stdio idle timeout
c. To backup the P-660R-F1 configurations, use TFTP client program to get file **"rom-0"** from the P-660R-F1.
d. To restore the P-660R-F1 configurations, use the TFTP client program to put your configuration in file **rom-0** in the P-660R-F1.

6. What should I do if I forget the system password?

In case you forget the system password, you can erase the current configuration and restore factory defaults this way:

Use the **RESET button** on the rear panel of P-660R-F1 to reset the router. After the router is reset, the LAN IP address will be reset to **'192.168.1.1',** the password will be reset to "**1234**"**.**

7. How to use the Reset button?

a. Turn your P-660R-F1 on. Make sure the **POWER** led is on (not blinking)
b. Press the **RESET** button for ten seconds **and** then release it. If the **POWER** LED begins to blink, the default configuration has been restored and the P-660R-F1 restarts.

8. What is SUA? When should I use SUA?

SUA (Single User Account) is a unique feature supported by P-660R-F1 router which allows multiple people to access Internet concurrently for the cost of a

All contents copyright © 2011 ZyXEL Communications Corporation.

single user account.

When P-660R-F1 acting as SUA receives a packet from a local client destined for the outside Internet, it replaces the source address in the IP packet header with its own address and the source port in the TCP or UDP header with another value chosen out of a local pool. It then recomputed the appropriate header checksums and forwards the packet to the Internet as if it is originated from P-660R-F1 using the IP address assigned by ISP. When reply packets from the external Internet are received by P-660R-F1, the original IP source address and TCP/UDP source port numbers are written into the destination fields of the packet (since it is now moving in the opposite direction), the checksums are recomputed, and the packet is delivered to its true destination. This is because SUA keeps a table of the IP addresses and port numbers of the local systems currently using it.

9. Is it possible to access a server running behind SUA from the outside Internet? How can I do it?

Yes, it is possible because P-660R-F1 delivers the packet to the local server by looking up to a SUA server table. Therefore, to make a local server accessible to the outside users, the port number and the inside IP address of the server must be configured. (You can configure it in Web Configurator, Advanced Setup, **Network -> NAT -> Port Forwarding**.

10. How many network users can the SUA/NAT support?

The **P-660R-F1** does not limit the number of the users but the number of the NAT sessions. The P-660R-F1 supports 1024 sessions.

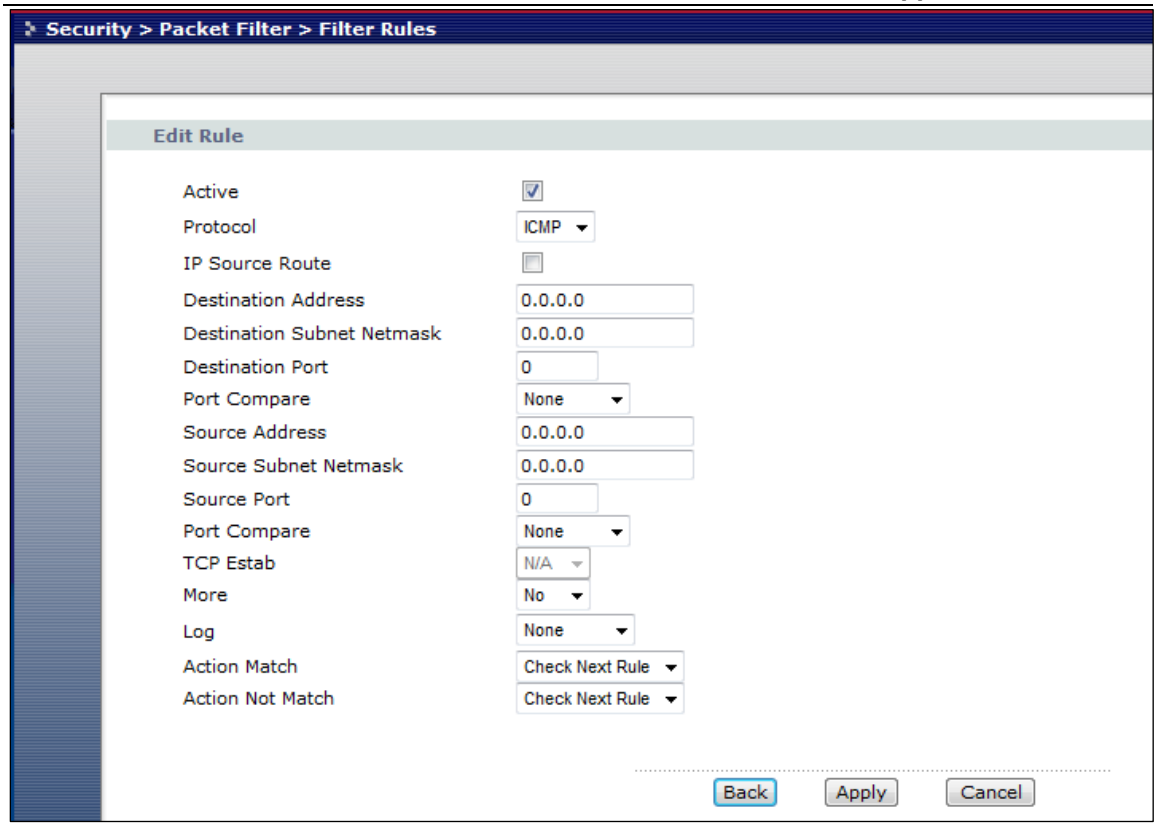
11. What are Device filters and Protocol filters?
In ZyNOS, the filters have been separated into two groups. One group is called 'device filter group', and the other is called 'protocol filter group'. Generic filters belong to the 'device filter group', TCP/IP and IPX filters belong to the 'protocol filter group'. You can configure the filter rule in **CLI**.
Note: In ZyNOS, you can not mix different filter groups in the same filter set.

12. How can I protect against IP spoofing attacks?

The P-660R-F1's filter sets provide a means to protect against IP spoofing attacks. The basic scheme is according to your need to set different filter type. There are two types of filter: Protocol Filter and Generic Filter.

For the rule setup:

All contents copyright © 2011 ZyXEL Communications Corporation.



All contents copyright © 2011 ZyXEL Communications Corporation.

Product FAQ

1. How can I manage P-660R-F1?

English Web GUI for Local and Remote management
CLI (Command-line interface)
Telnet support (Administrator Password Protected) for remote configuration change and status monitoring
FTP server, firmware upgrade and configuration backup and restore are Supported (Administrator Password Protected)

2. What is the default password for Web Configurator?

By factory default the password for P-660R-F1 Web Configurator is **1234**. You can login in as an administrator. You can change the password after you logging in the Web Configurator.
Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.

3. How do I know the P-660R-F1's WAN IP address assigned by the ISP?

You can view **" IP Address<from ISP>: x.x.x.x"** shown in Web Configurator **Status->Device Information ->WAN Infomation"** to check this IP address.

4. What is Traffic Shaping?

Traffic Shaping allocates the bandwidth to WAN dynamically and aims at boosting the efficiency of the bandwidth. If there are several VCs in the P-660R-F1 but only one VC activated at one time, the P-660R-F1 allocates all the Bandwidth to the VC and the VC gets full bandwidth. If another VCs are activated later, the bandwidth is yield to other VCs after ward.

5. Why do we perform traffic shaping in the P-660R-F1?

The P-660R-F1 must manage traffic fairly and provide bandwidth allocation for different sorts of applications, such as voice, video, and data. All applications have their own natural bit rate. Large data transactions have a fluctuating natural bit rate. The P-660R-F1 is able to support variable traffic among different virtual connections. Certain traffic may be discarded if the virtual connection experiences congestion. Traffic shaping defines a set of actions taken by the P-660R-F1 to avoid congestion; traffic shaping takes measures to adapt to unpredictable fluctuations in traffic flows and other problems among virtual connections.

6. What do the parameters (PCR, SCR, and MBS) mean?

Traffic shaping parameters (**PCR, SCR, MBS**) can be set in Web Configurator, **Network -> WAN -> Internet Connection -> Advanced Setup -> ATM QoS**:

All contents copyright © 2011 ZyXEL Communications Corporation.

Peak Cell Rate (PCR): The maximum bandwidth allocated to this connection. The VC connection throughput is limited by PCR.

Sustainable Cell Rate (SCR): The least guaranteed bandwidth of a VC. When there are multi-VCs on the same line, the VC throughput is guaranteed by SCR.

Maximum Burst Size(MBS): The amount of cells transmitted through this VC at the Peak Cell Rate before yielding to other VCs. Total bandwidth of the line is dedicated to single VC if there is only one VC on the line. However, as the other VC asking the bandwidth, the MBS defines the maximum number of cells transmitted via this VC with Peak Cell rate before yielding to other VCs.

The P-660R-F1 holds the parameters for shaping the traffic among its virtual channels. If you do not need traffic shaping, please set SCR = 0, MBS = 0 and PCR as the maximum value according to the line rate (for examp le, 2.3 Mbps line rate will result PCR as 5424 cell/sec.)

7. What do the ATM QoS Types (CBR, UBR, VBR, rtVBR, nrtVBR) mean?

Constant bit rate (CBR): An ATM bandwidth-allocation service that requires the user to determine a fixed bandwidth requirement at the time the connection is set up so that the data can be sent in a steady stream. CBR service is often used when transmitting fixed-rate uncompressed video.

Unspecified bit rate (UBR): An ATM bandwidth-allocation service that does not guarantee any throughput levels and uses only available bandwidth. UBR is often used when transmitting data that can tolerate delays, such as e-mail.

Variable bit rate (VBR): An ATM bandwidth-allocation service that allows users to specify a throughput capacity (i.e., a peak rate) and a sustained rate but data is not sent evenly. You can select VBR for burst traffic and bandwidth sharing with other applications. It contains two subclasses:

Non-real time variable bit rate (nrtVBR) and **Real time variable bit rate (rtVBR).**

8. The P-660R-F1 supports Bridge and Router mode, what's the difference between them?

When the ISP limits some specific computers to access Internet that means only the traffic to/from these computers will be forwarded and the other will be filtered. In this case, we use bridge mode which works as an ADSL modem to connect to the ISP. The ISP will generally give one Internet account and limit only one computer to access the Internet.

For most Internet users having multiple computers want to share an Internet account for Internet access, they have to add another Internet sharing device, like

All contents copyright © 2011 ZyXEL Communications Corporation.

a router. In this case, we use the router mode which works as a general Router plus an ADSL Modem.

9. How do I know I am using PPPoE?

PPPoE requires a user account to login to the provider's server. If you need to configure a user name and password on your computer to connect to the ISP you are probably using PPPoE. If you are simply connected to the Internet when you turn on your computer, you probably are not. You can also check your ISP or the information sheet given by the ISP. Please choose PPPoE as the encapsulation type in the P-660R-F1 if the ISP uses PPPoE.

10. Why does my provider use PPPoE?

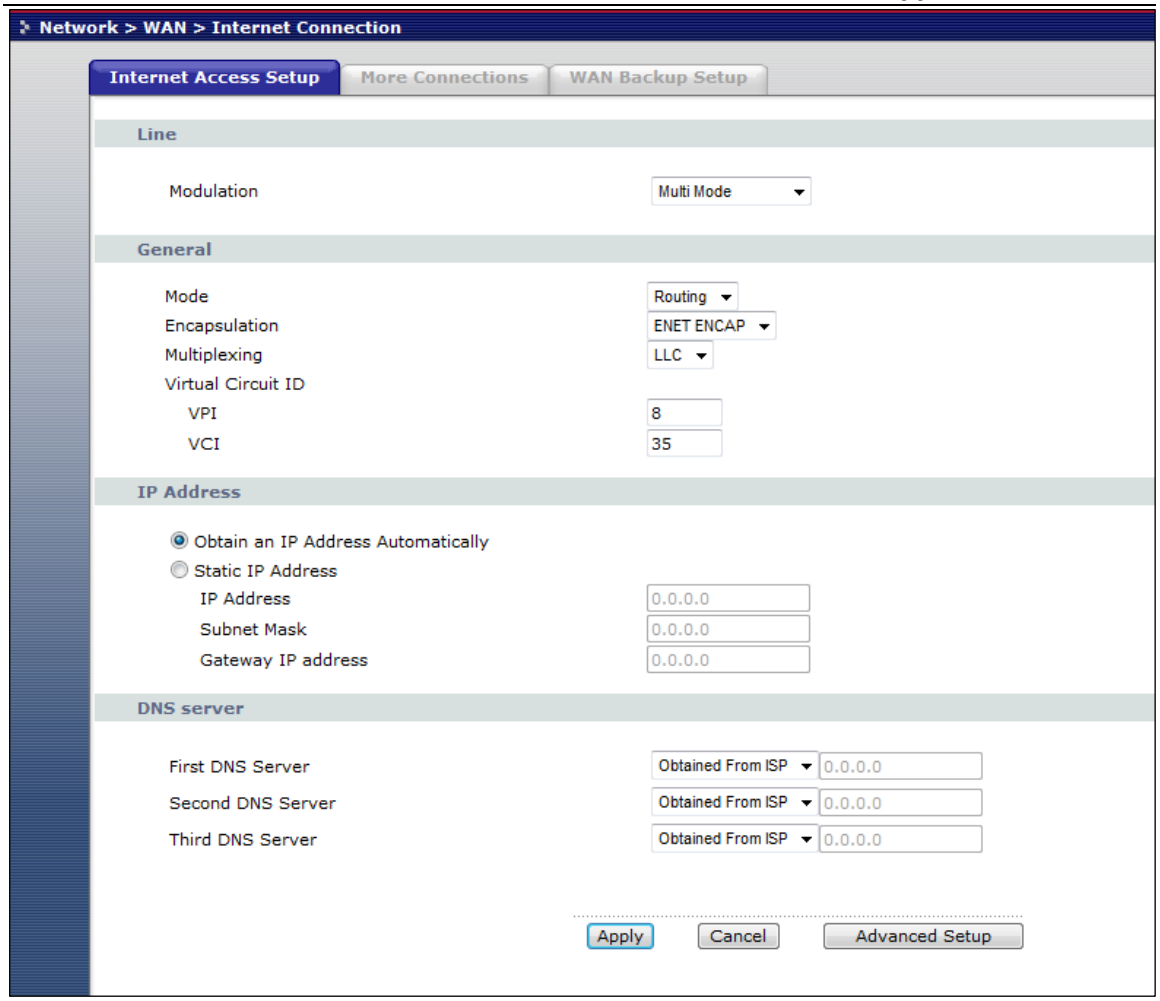
PPPoE emulates a familiar Dial-Up connection. It allows your ISP to provide services using their existing network configuration over the broadband connections. Besides, PPPoE supports a broad range of existing applications and service including authentication, accounting, secure access and configuration management.

11. When do I need to choose dynamic IP?

If your ISP provides you an IP address automatically, typically used for Cable service. In this case your computer gets an IP dynamically assigned by DHCP.

To use this mode, you need to do some corresponding configurations on the web page: **Network -> WAN -> Internet Connection**:

All contents copyright © 2011 ZyXEL Communications Corporation.



Key setting:

Option	Description
Encapsulation	Select the correct Encapsulation type that your ISP supports. For example, RFC 1483.
Multiplexing	Select the correct Multiplexing type that your ISP supports. For example, LLC.
VPI & VCI number	Specify a VPI (Virtual Path Identifier) and a VCI (Virtual Channel Identifier) given to you by your ISP.

All contents copyright © 2011 ZyXEL Communications Corporation.

12. What is DDNS?

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname, allowing your computer to be more easily accessed from various locations on the Internet. To use the service, you must first apply an account from several free Web servers such as http://www.dyndns.org/.

Without DDNS, we always tell the users to use the WAN IP of the P-660R-F1 to reach our internal server. It is inconvenient for the users if this IP is dynamic. With DDNS supported by the P-660R-F1, you apply a DNS name (e.g., www.zyxel.com.tw) for your server (e.g., Web server) from a DDNS server. The outside users can always access the web server using the www.zyxel.com.tw regardless of the WAN IP of the P-660R-F1.

When the ISP assigns the P-660R-F1 a new IP, the P-660R-F1 updates this IP to DDNS server so that the server can update its IP -to-DNS entry. Once the IP-to-DNS table in the DDNS server is updated, the DNS name for your web server (i.e., www.zyxel.com.tw) is still usable.

13. When do I need DDNS service?

When you want your internal server to be accessed by using DNS name rather than using the dynamic IP address we can use the DDNS service. The DDNS server allows to alias a dynamic IP address to a static hostname. Whenever the ISP assigns you a new IP, the P-660R-F1 sends this IP to the DDNS server for its updates.

14. What is DDNS wildcard? Does the P-660R-F1 support DDNS wildcard?

Some DDNS servers support the wildcard feature which allows the hostname, *.yourhost.dyndns.org, to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful when there are multiple servers inside and you want users to be able to use things such as www.yourhost.dyndns.org and still reach your hostname.

Yes, the P-660R-F1 supports DDNS wildcard that http://www.dyndns.org/ supports. And you can choose to active or inactive this feature on the web configuration page. When using wildcard, you simply enter yourhost.dyndns.org on the web configuration page.

15. Can the P-660R-F1's SUA (Simple IP) handle IPSec packets sent by the IPSec gateway?

Yes, the P-660R-F1's SUA can handle IPSec ESP Tunneling mode. We know when packets go through SUA; SUA will change the source IP address and source port for the host. To pass IPSec packets, SUA must understand the ESP packet with protocol number 50; replace the source IP address of the IPSec gateway to the router's WAN IP address. However, SUA should not change the

All contents copyright © 2011 ZyXEL Communications Corporation.

source port of the UDP packets which are used for key managements. Because the remote gateway checks this source port during connections, the port thus is not allowed to be changed.

16. What is UPnP?

Universal Plug and Play (UPnP) is a set of computer network protocols promulgated by the UPnP Forum. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and corporate environments. UPnP achieves this by defining and publishing UPnP device control protocols built upon open, Internet-based communication standards.

All contents copyright © 2011 ZyXEL Communications Corporation.

ADSL FAQ

1. How does ADSL compare to Cable modems?

ADSL provides a dedicated service over a single telephone line; cable modems offer a dedicated service over a shared media. While cable modems have greater downstream bandwidth capabilities (up to 30 Mbps), that bandwidth is shared among all users on a line, and will therefore vary, perhaps dramatically, as more users in a neighborhood get online at the same time. Cable modem upstream traffic will in many cases be slower than ADSL, either because the particular cable modem is inherently slower, or because o f rate reductions caused by contention for upstream bandwidth slots. The big difference between ADSL and cable modems, however, is the number of lines available to each. There are no more than 12 million homes passed today that can support two-way cable modem transmissions, and while the figure also grows steadily, it will not catch up with telephone lines for many years. Additionally, many of the older cable networks are not capable of offering a return channel; consequently, such networks will need significant upgrading before they can offer high bandwidth services.

2. What is the micro-filter or splitter used for?

Generally, the voice band uses the lower frequency ranging from 0 to 4KHz, while ADSL data transmission uses the higher frequency. The micro filter acts as a low-pass filter for your telephone set to ensure that ADSL transmissions do not interfere with your voice transmissions. For the details about how to connect the micro filter please refer to the user's manual.

3. How do I know the ADSL line is up?

You can see the DSL LED Green on the P-660R-F1's front panel is on when the ADSL physical layer is up.

4. How does the P-660R-F1 work on a noisy ADSL?

Depending on the line quality, the P-660R-F1 uses “Fall Back” and “Fall Forward” to automatically adjust the data rate.

5. Does the VC-based multiplexing perform better than the LLC-based multiplexing?

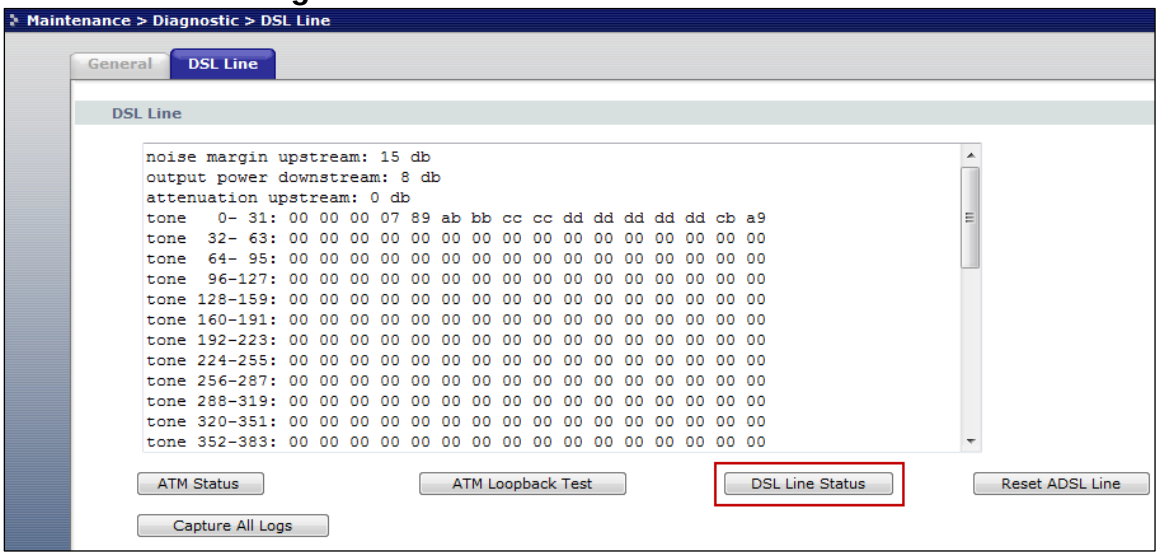
Though the LLC-based multiplexing can carry multiple protocols over a single VC, it requires extra header information to identify the protocol being carried on the virtual circuit (VC). The VC -based multiplexing needs a separate VC for carrying each protocol but it does not need the extra headers. Therefore, the VC-based multiplexing is more efficient.

We can choose one of them on the web configuration page: **Network -> WAN -> Internet Connection -> Multiplexing.**

All contents copyright © 2011 ZyXEL Communications Corporation.

6. How do I know the details of my ADSL line statistics?

You can use the following CI commands to check the ADSL line statistics. CI> CI> wan adsl perfdata
CI> wan adsl status
CI> wan adsl linedata far
CI> wan adsl linedata near
You can also do it in Web Configurator, Advanced Setup,
Maintenance -> Diagnostic -> DSL Line -> DSL Line Status:



7. What are the signaling pins of the ADSL connector?

The signaling pins on the P-660R-F1's ADSL connector are pin 3 and pin 4. The middle two pins for a RJ11 cable.

All contents copyright © 2011 ZyXEL Communications Corporation.

Application Notes

General Application Notes

1. Internet Access Using P-660R-F1 under Bridge mode

Setup your workstation
Setup your P-660R-F1 under bridge mode

If the ISP limits some specific computers to access Internet, that means only the traffic to/from these computers will be forwarded and the other will be filtered. In this case, we use P-660R-F1 which works as an ADSL bridge modem to connect to the ISP. The ISP will generally give one Internet account and limit only one computer to access the Internet. See the figure below for this setup:

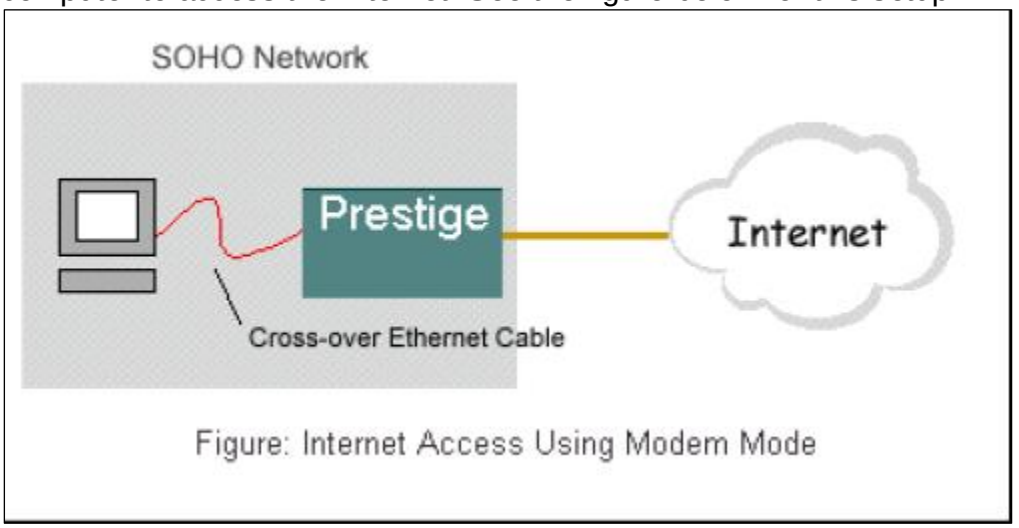


Figure: Internet Access Using Modem Mode

Set up your workstation

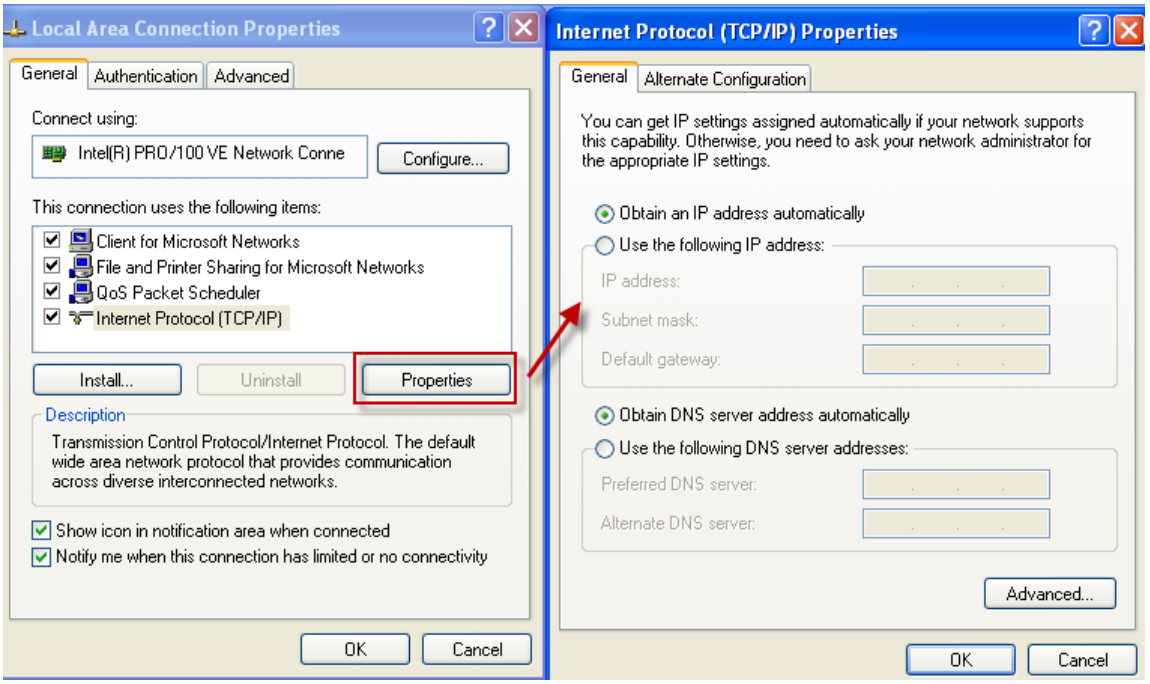
(1) Ethernet connection

To connect your computer to the P-660R-F1's LAN port, the computer must have an Ethernet adapter card installed. For connecting a single computer to the P-660R-F1, we use an Ethernet cable.

(2) TCP/IP configuration

In most cases, the IP address of the computer is assigned by the ISP dynamically so you have to configure the computer as a DHCP client which obtains the IP from the ISP using DHCP protocol. The ISP may also provide the gateway, DNS via DHCP if they are available. Otherwise, please enter the static IP addresses for all that the ISP gives to you in the network TCP/IP settings. For Windows, we check the option ***'Obtain an IP address automatically'*** in its TCP/IP setup, please see the example shown below.

All contents copyright © 2011 ZyXEL Communications Corporation.

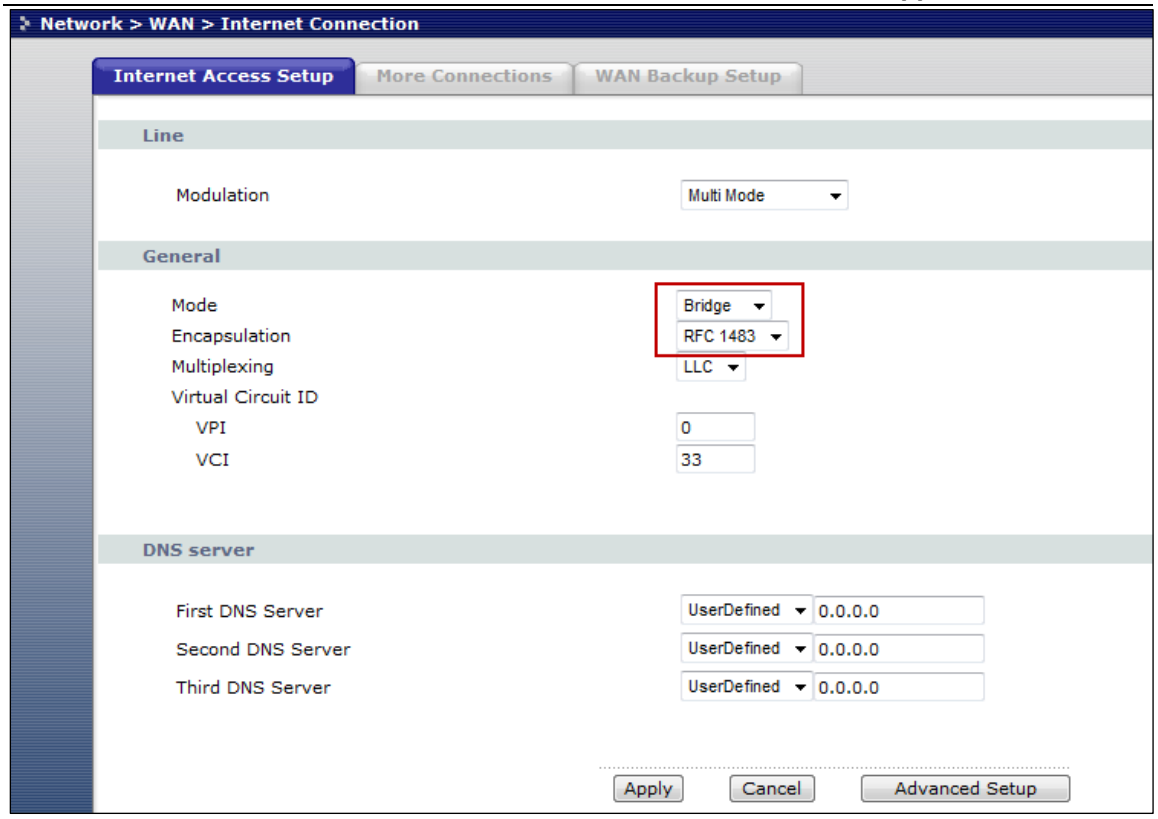

Local Area Connection Properties
General
Authentication
Advanced
Connect using:
Intel(R) PRO/100 VE Network Conne
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Internet Protocol (TCP/IP)
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in notification area when connected
Notify me when this connection has limited or no connectivity
OK
Cancel
Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Setup your P-660R-F1 under bridge mode

The following procedure shows you how to configure your P-660R-F1 as bridge mode. We will use Web Configurator to guide you through the related menu.

(1) Configure P-660R-F1 as bridge mode and configure Internet setup parameters in Web Configurator, Advanced Setup. **Network -> WAN -> Internet Connection.**

All contents copyright © 2011 ZyXEL Communications Corporation.



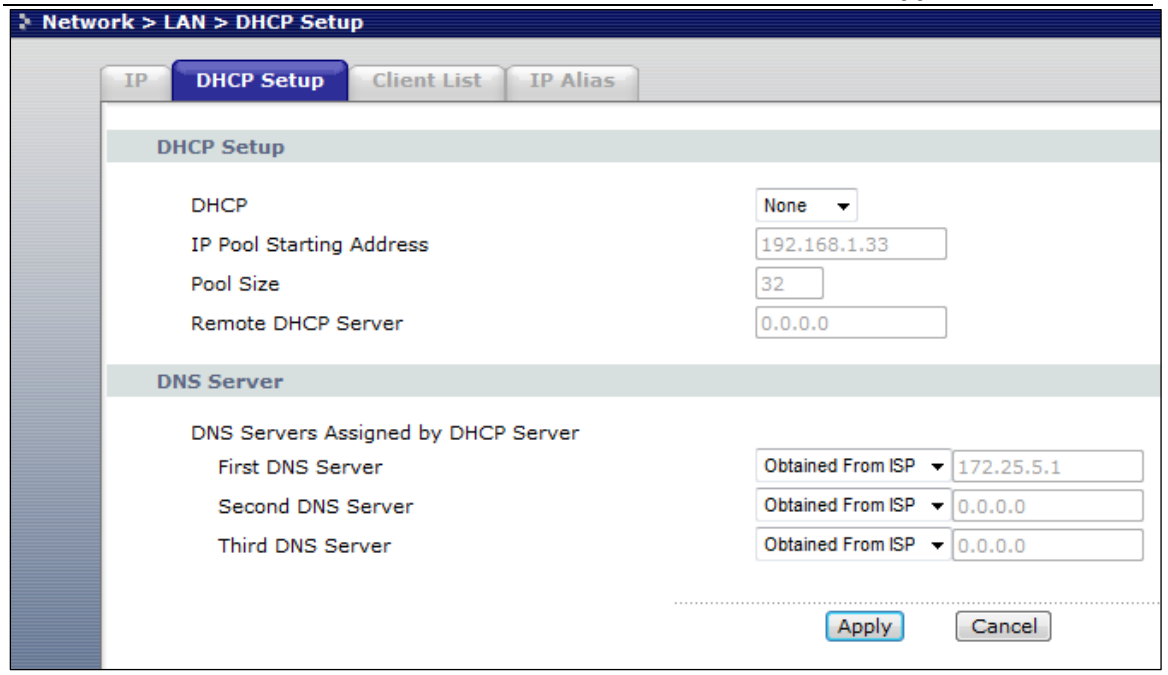
Key Settings:

Option	Description
Encapsulation	Select the correct Encapsulation type that your ISP supports. For example, RFC 1483.
Multiplexing	Select the correct Multiplexing type that your ISP supports. For example, LLC.
VPI & VCI number	Specify a VPI (Virtual Path Identifier) and a VCI (Virtual Channel Identifier) given to you by your ISP.

(2) Turn off DHCP Server and configure a LAN IP for the P-660R-F1 in Web Configurator, Advanced Setup, Interface Setup -> LAN -> DHCP.. We use 192.168.1.1 as the LAN IP for P-660R-F1 in this case:

Step 1: Disable DHCP Server and save it:
Step 2: Assign an IP to the LAN Interface of P-660R-F1, e.g.: 192.168.1.1:

All contents copyright © 2011 ZyXEL Communications Corporation.



2. Internet Access Using P-660R-F1 under Routing mode

For most Internet users having multiple computers want to share an Internet account for Internet access, they have to install an Internet sharing device, like a router. In this case, we use the P-660R-F1 which works as a general Router plus an ADSL Modem.

Set up your workstation

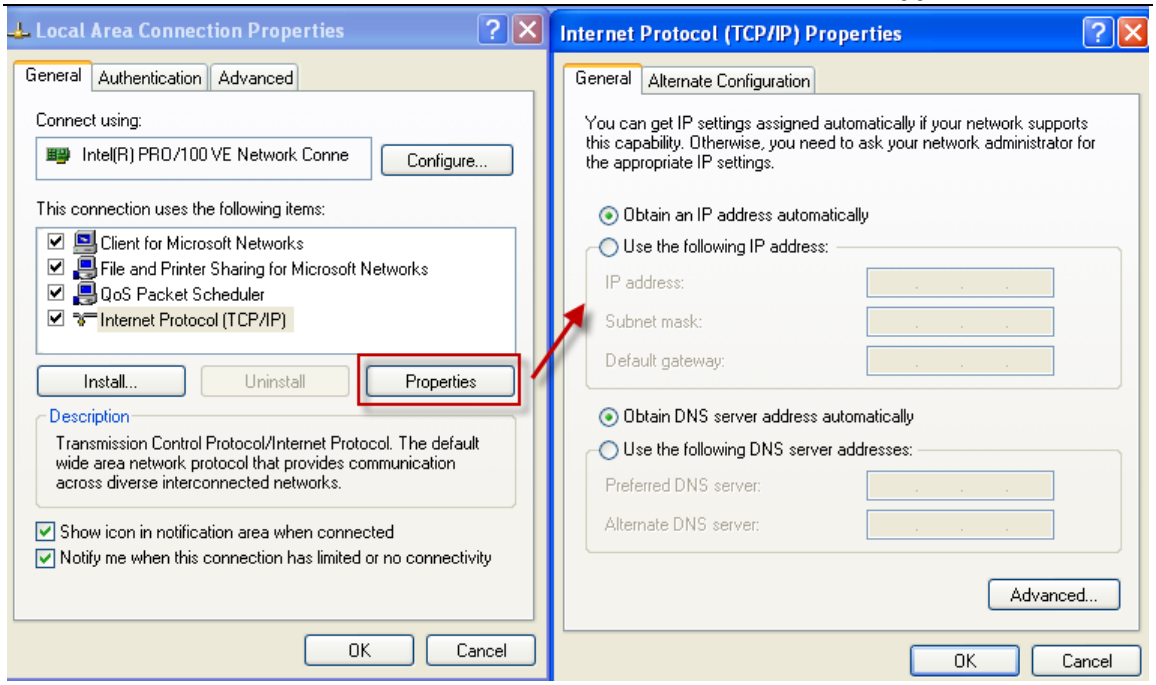
(1) Ethernet connection

Connect the LAN ports of all computers to the LAN Interface of P-660R-F1 using Ethernet cable.

(2) TCP/IP configuration

Since the P-660R-F1 is set to DHCP server as default, so you need only to configure the workstations as the DHCP clients in the networking settings. In this case, the IP address of the computer is assigned by the P-660R-F1.
The P-660R-F1 can also provide the DNS to the clients via DHCP if it is available.
For this setup in Windows, we check the option ***'Obtain an IP address automatically'*** in its TCP/IP setup. Please see the example shown below.

All contents copyright © 2011 ZyXEL Communications Corporation.

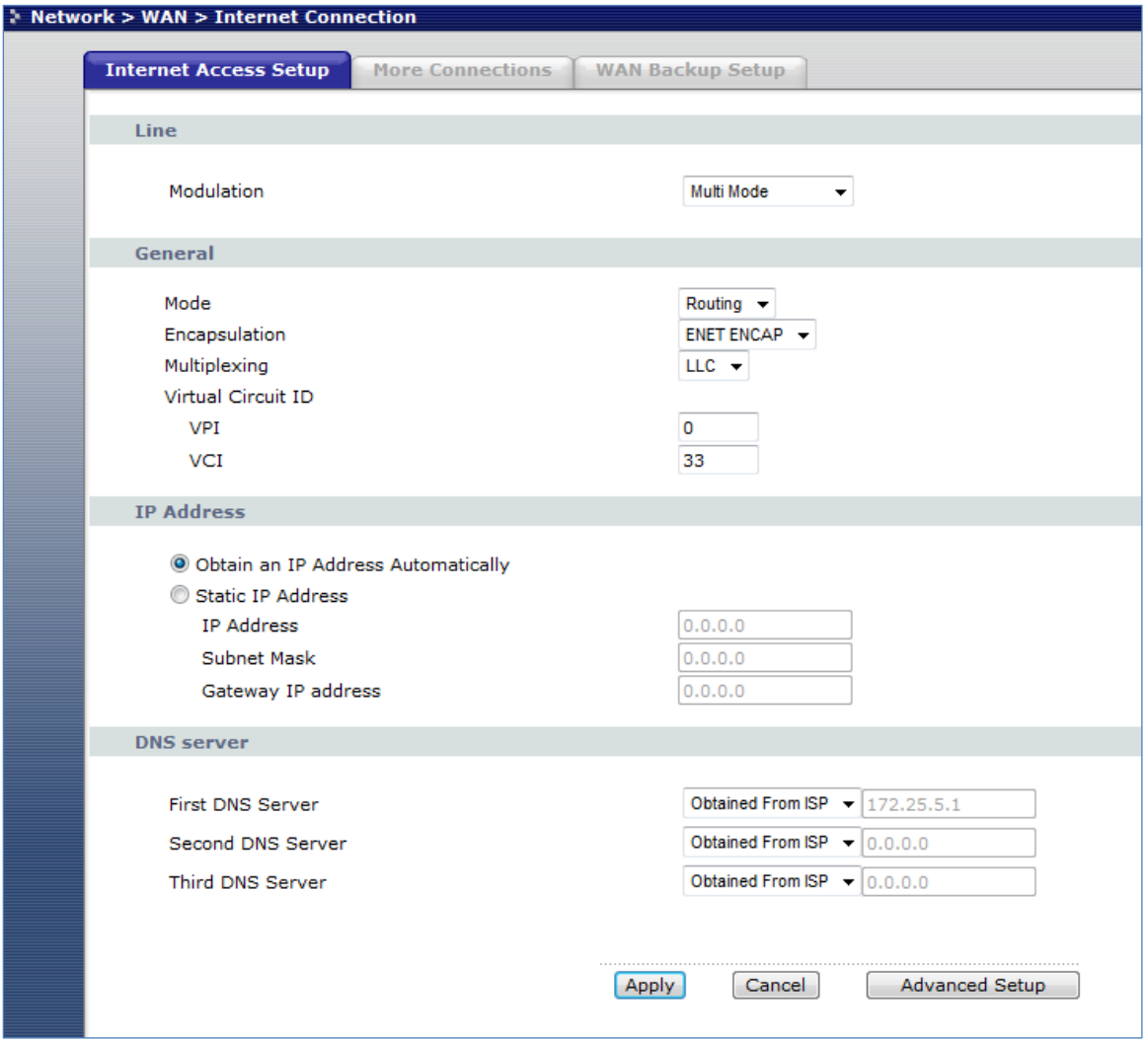

Local Area Connection Properties
General
Authentication
Advanced
Connect using:
Intel(R) PRO/100 VE Network Conne
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Internet Protocol (TCP/IP)
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in notification area when connected
Notify me when this connection has limited or no connectivity
OK
Cancel
Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Set up your P-660R-F1 under routing mode

The following procedure shows you how to configure your P-660R-F1 as Routing mode for routing traffic. We will use Web Configurator to guide you through the related menu.

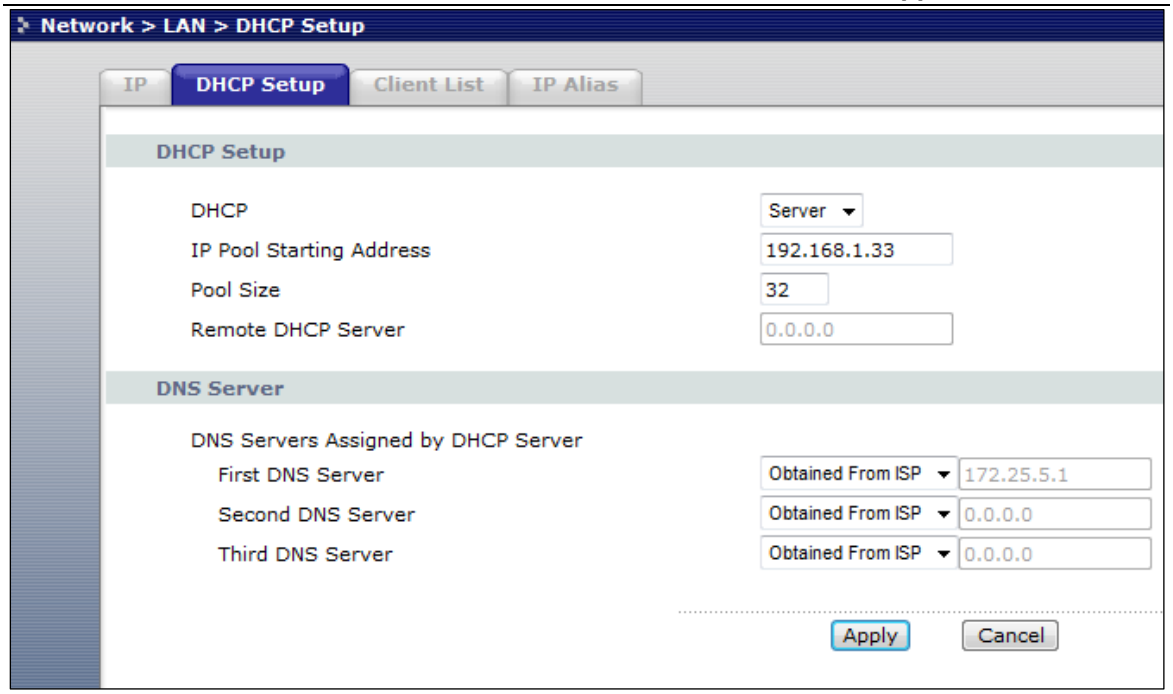
(1) Configure P-660R-F1 as routing mode and configure Internet setup parameters in Web Configurator, Advanced Setup, **Network -> WAN -> Internet Connection.**

All contents copyright © 2011 ZyXEL Communications Corporation.



(2) Configure a LAN IP for the P-660R-F1 and the DHCP settings in Web Configurator, Advanced Setup, **Network -> LAN -> DHCP Setup.**

All contents copyright © 2011 ZyXEL Communications Corporation.



3. Setup the P-660R-F1 as a DHCP Relay

What is DHCP Relay?

DHCP stands for Dynamic Host Configuration Protocol. In addition to the DHCP server feature, the P-660R-F1 supports the DHCP relay function. When it is configured as DHCP server, it assigns the IP addresses to the LAN clients. When it is configured as DHCP relay, it is responsible for forwarding the requests and responses negotiating between the DHCP clients and the server. Please see below figure.

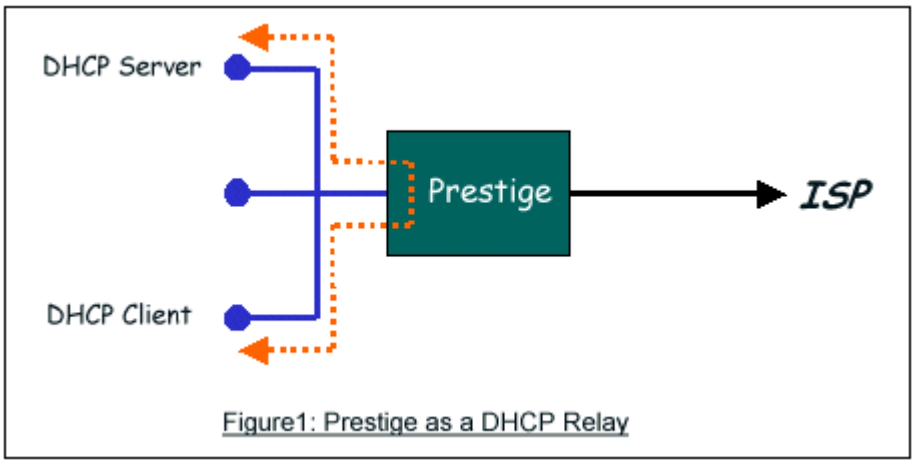


Figure1: Prestige as a DHCP Relay

Prestige means P-660R-F1.

Setup the P-660R-F1 as a DHCP Relay

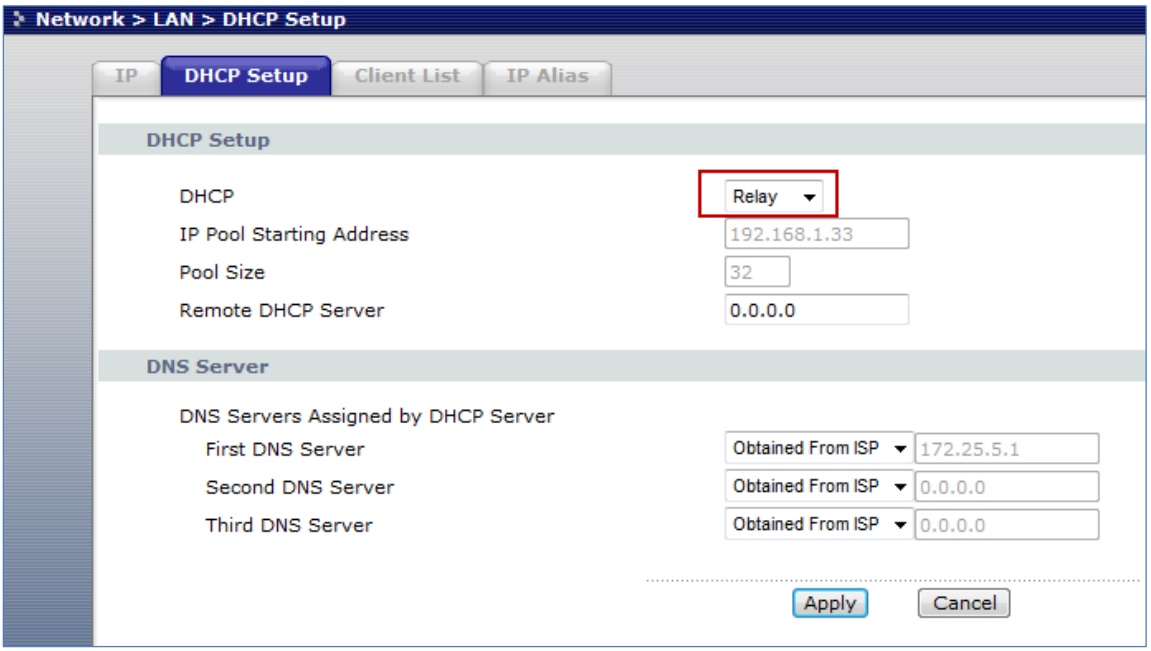
We could set the P-660R-F1 as a DHCP Relay by the following command in **CLI**:

Ip dhcp enif0 relay

All contents copyright © 2011 ZyXEL Communications Corporation.

Ip dhcp enif0 relay server [Server IP Address]

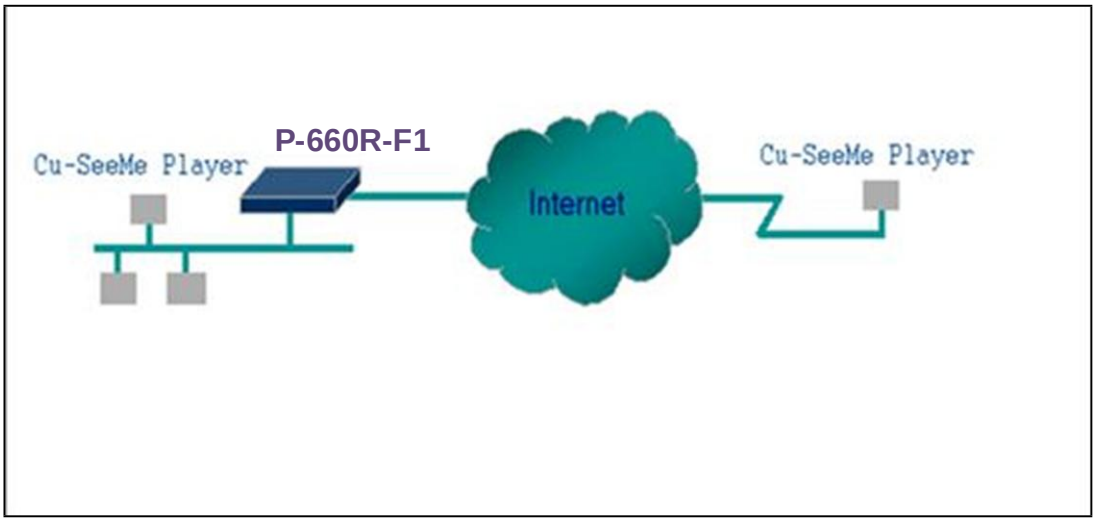
You can also set it in web configuration page: **Interface Setup -> LAN -> DHCP.**



Click to choose “Relay”, input the Remote DHCP Server and click Apply button.

4. SUA Notes

Tested SUA/NAT Applications (e.g., Cu-SeeMe, ICQ, NetMeeting)



Introduction

Generally, SUA makes your LAN appear as a single machine to the outside world. LAN users are invisible to outside users. However, some applications such as Cu-SeeMe and ICQ will need to connect to the local user behind the P-660R-F1. In such case, a SUA server must be configured to forward the incoming packets to

All contents copyright © 2011 ZyXEL Communications Corporation.

the true destination behind SUA. After the required server are configured in Web Configurator, Advanced Setup, **Network -> NAT -> Port Forwarding,** the internal server or client applications can be accessed by using the P-660R-F1's ***WAN IP* Address**.

SUA Supporting Table

The following are the required Web Configurator, Advanced Setup, **Network -> NAT -> Port Forwarding** for the various applications running in Single mode.

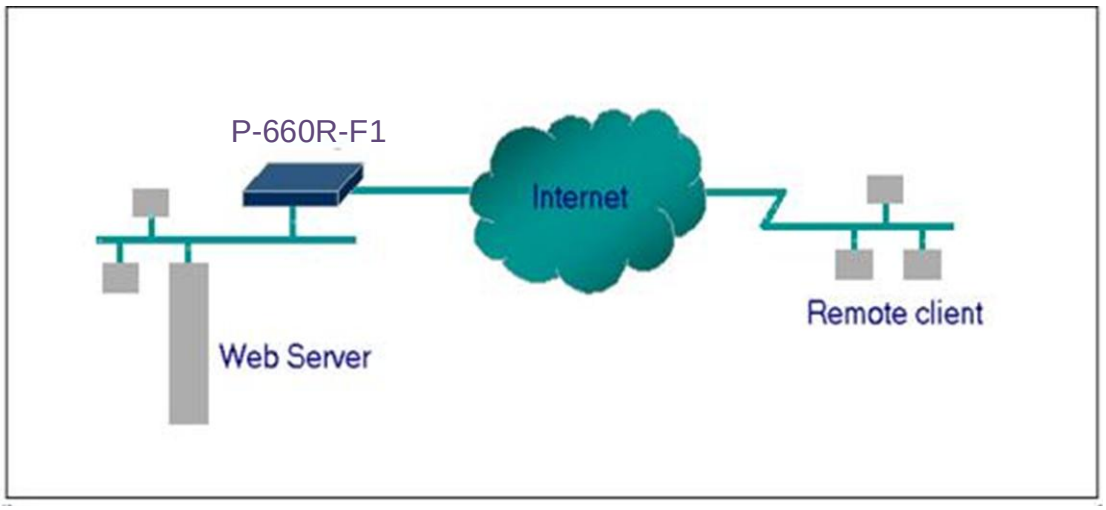
Application	Required Settings in **Port Forwarding** Port/IP	
	Outgoing Connection	Incoming Connection
FTP	None	21/client IP
SSH	None	22/client IP
TELNET	None	23/client IP (and active Telnet service from WAN)
E-mail (SMTP)	None	25/client IP
WWW	None	80/client IP
E-maile (POP3)	None	110/client IP
HTTPs	None	443/client IP
T.120	None	1503/client IP
H.232	None	1720/client IP
PPTP	None	1723/client IP
pcAnywhere	None	5631/client IP
VNC	None	5900/client IP
CUSeeMe	None	7648/client IP
mIRC	None for Chat. For DCC, please set Default/Client IP	
ICQ 99a	None for Chat. For DCC, please set: ICQ -> preference -> connections -> firewall and set the firewall time out to 80 seconds in firewall setting.	Default/client IP
ICQ 2000b	None for Chat	None for Chat
ICQ Phone 2000b	None	6701/client IP

All contents copyright © 2011 ZyXEL Communications Corporation.

IPsec (ESP tunneling mode)	None (one client only)	Default/Client
Microsoft Messenger Service 3.0	6901/client IP	6901/client IP
Microsoft Messenger Service 4.6/ 4.7/ 5.0/… (none UPnP)	None for Chat, File transfer ,Video and Voice	None for Chat, File transfer, Video and Voice
Remote Anything	None	3996 - 4000/client IP
Virtual Network Computing (VNC)	None	5500/client IP 5800/client IP 5900/client IP

Configurations

Configure an Internal Server behind SUA



Introduction

If you wish, you can make internal servers (e.g., Web, ftp or mail server) accessible for outside users, even though SUA makes your LAN appear as a single machine to the outside world. A service is identified by the port number. Also, since you need to specify the IP address of a server behind the P-660R-F1, a server must have a fixed IP address and not be a DHCP client whose IP address potentially changes each time P-660R-F1 is powered on.
In addition to the servers for specific services, SUA supports a default server. A service request that does not have a server explicitly designated for is forwarded to the default server. If the default server is not defined, the service request is simply discarded.

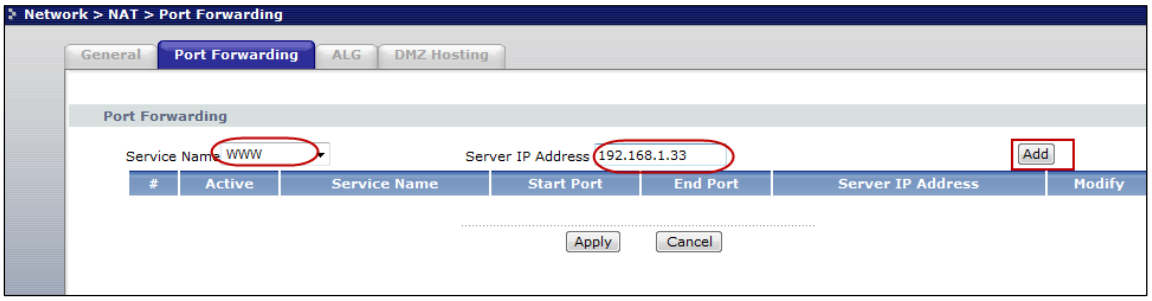
All contents copyright © 2011 ZyXEL Communications Corporation.

Configuration

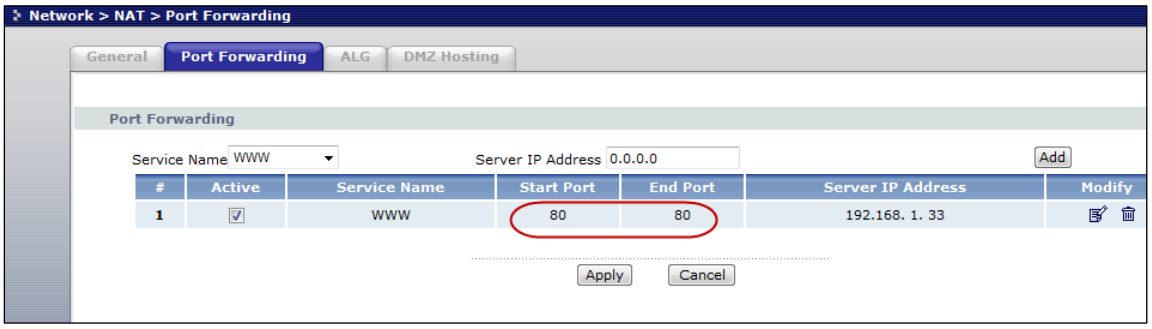
To make a server visible to the outside world, specify the port number of the service and the inside address of the server in Web Configurator, Advanced Setup, **Network -> NAT -> Port Forwarding.** The outside users can access the local server using the P-660R-F1's ***WAN IP*** address which can be obtained from Web Configurator, **Status -> WAN Information**.
For example:

Configuring an internal Web server for outside access (suppose the Server IP Address is 192.168.1.33):

(1) Fill in the service name and server IP Address, press button 'Add'



(2) If add successfully, the Web Configurator will display message 'Configuration updated successfully' at the bottom. You can see the port forwarding rule on the same page, the default port for Web Server is 80:



(3) If you want to change the port for Web Server, you could press button 'Modify' on corresponding rule, then modify and apply it.

Default port numbers for some services

Service	Port Number
FTP	21
Telnet	23
SMTP	25

All contents copyright © 2011 ZyXEL Communications Corporation.

DNS (Domain Name Server)	53
www-http (Web)	80
POP3	110
HTTPs	443
PPTP	1723

Configure a PPTP server behind SUA

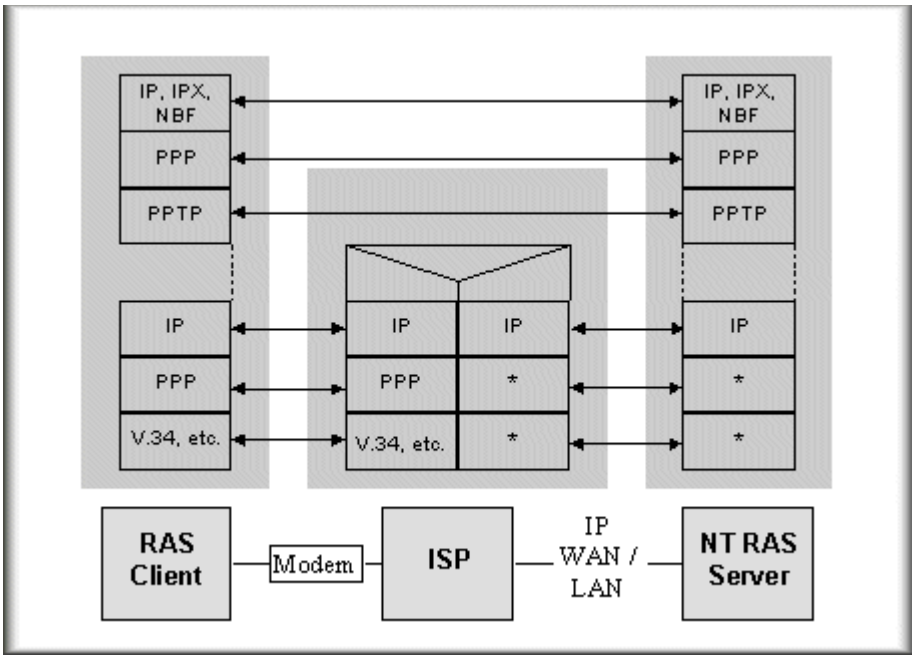
Introduction

PPTP is a tunneling protocol defined by the PPTP forum that allows PPP packets to be encapsulated within Internet Protocol (IP) packets and forwarded over any IP network, including the Internet itself.

In order to run the Windows 9x PPTP client, you must be able to establish an IP connection with a tunnel server such as the Windows NT Server 4.0 Remote Access Server.

Windows Dial-Up Networking uses the Internet standard Point-to-Point (PPP) to provide a secure, optimized multiple-protocol network connection over dial-up telephone lines. All data sent over this connection can be encrypted and compressed, and multiple network level protocols (TCP/IP, NetBEUI and

IPX) can be run correctly. Windows NT Domain Login level security is preserved even across the Internet.



Window98 PPTP Client / Internet / NT RAS Server Protocol Stack

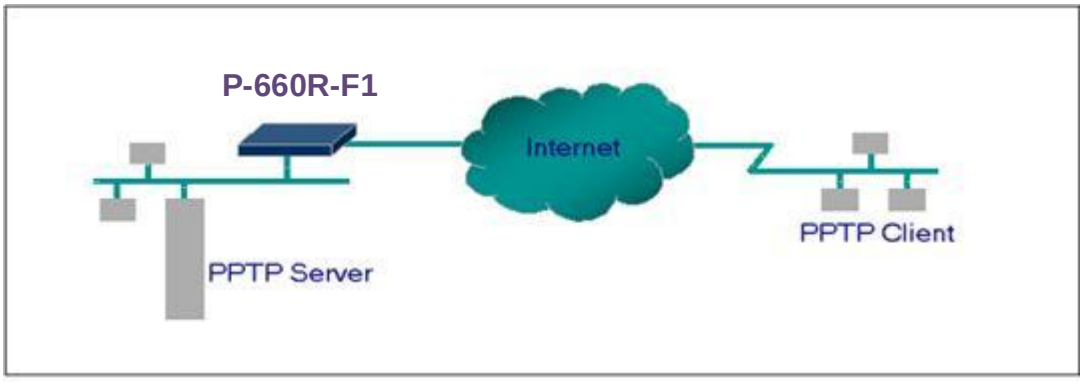
All contents copyright © 2011 ZyXEL Communications Corporation.

PPTP appears as new modem type (Virtual Private Networking Adapter) that can be selected when setting up a connection in the D ial-Up Networking folder. The VPN Adapter type does not appear elsewhere in the system. Since PPTP encapsulates its data stream in the PPP protocol, the VPN requires a second dial-up adapter. This second dial-up adapter for VPN is added during the installation phase of the Upgrade in addition to the first dial -up adapter that provides PPP support for the analog or ISDN modem.

The PPTP is supported in Windows NT and Windows 98 already. For Windows 95, it needs to be upgraded by the Dial-Up Networking 1.2 upgrade.

Configuration

This application note explains how to establish a PPTP connection with a remote private network in the P-660R-F1 SUA case. By default, the port number of the PPTP is 1723.



Example

The following example shows how to dial to an ISP via the P-660R-F1 and then establish a tunnel to a private network. There will be three items that you need to set up for PPTP application, these are PPTP server (WinNT), PPTP client (Win9x) and the P-660R-F1.

(1) PPTP server setup (WinNT)

Add the VPN service from Control Panel ->Network
Add an user account for PPTP logged on user
Enable RAS port
Select the network protocols from RAS such as IPX, TCP/IP NetBEUI
Set the Internet gateway to P-660R-F1

(2) PPTP client setup (Win9x)

Add one VPN connection from Dial-Up Networking by entering the correct username & password and the IP address of the P-660R-F1's Internet IP address for logging to NT RAS server.
Set the Internet gateway to the router that is connecting to ISP

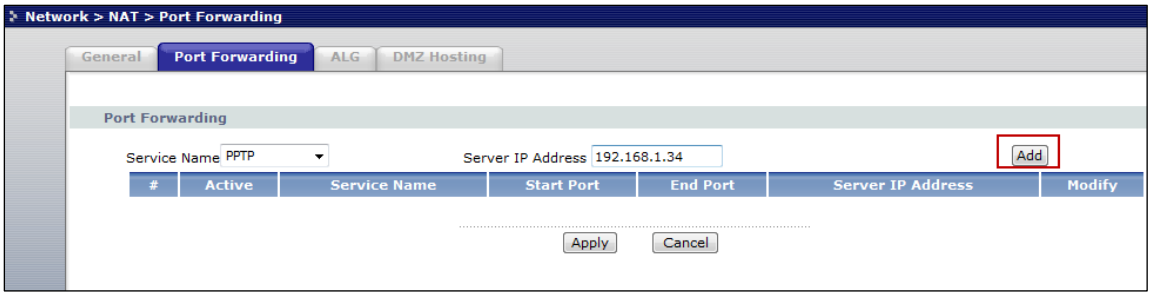
All contents copyright © 2011 ZyXEL Communications Corporation.

(3) P-660R-F1 setup

Before making a VPN connection from Win9x to WinNT server, you need to connect P-660R-F1 router to your ISP first.

Enter the IP address of the PPTP server (WinNT server) and the port number for PPTP as shown below:

Select service name as „PPTP" , fill in the Server IP Address, then press button "Save".



When you have finished the above settings, you can ping to the remote Win9x client from WinNT. This ping command is used to demonstrate that remote the Win9x can be reached across the Internet. If the Internet connection between two LANs is achievable, you can place a VPN call from the remote Win9x client.

For example: C:\ping 203.66.113.2

When a dial-up connection to ISP is established, a default gateway is assigned to the router traffic through that connection. Therefore, the output below shows the default gateway of the Win9x client after the dial-up connection has been established.

Before making a VPN connection from the Win9x client to the NT server, you need to know the exact Internet IP address that the ISP assigns to P-660R-F1 router in SUA mode and enter this IP address in the VPN dial-up dialog box.
You can check this Internet IP address from PNC Monitor or S Web Configurator, **Status -> WAN Information.** If the Internet IP address is a fixed IP address provided by ISP in SUA mode, then you can a lways use this IP address for reaching the VPN server.

In the following example, the IP address '140.113.1.225' is dynamically assigned by ISP. You must enter this IP address in the 'VPN Server' dialog box for reaching the PPTP server. After the VPN link is established, you can start the network protocol application such as IP, IPX and NetBEUI.

All contents copyright © 2011 ZyXEL Communications Corporation.

NAT Server Sets

The NAT Server Set is a list of LAN side servers mapped to external ports. If you wish, you can make inside servers for different services, e.g., Web or FTP, visible to the outside users, even though NAT makes your network appears as a single machine to the outside world. A server is identified by the port number, e.g., Web service is on port 80 and FTP on port 21.

As an example (see the following figure), if you have a Web server at 192.168.1.36 and a FTP server at 192.168.1.33, then you need to specify for port 80 (Web) the server at IP address 192.168.1.36 and for port 21 (FTP) another at IP address 192.168.1.33.

Please note that a server can support more than one service, e.g., a server can provide both FTP and Mail service, while another provides only Web service.

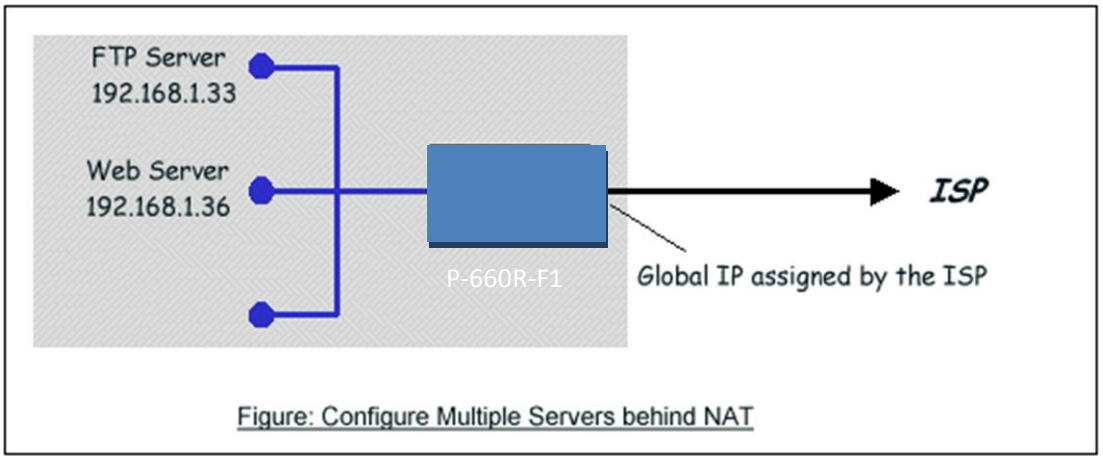


Figure: Configure Multiple Servers behind NAT

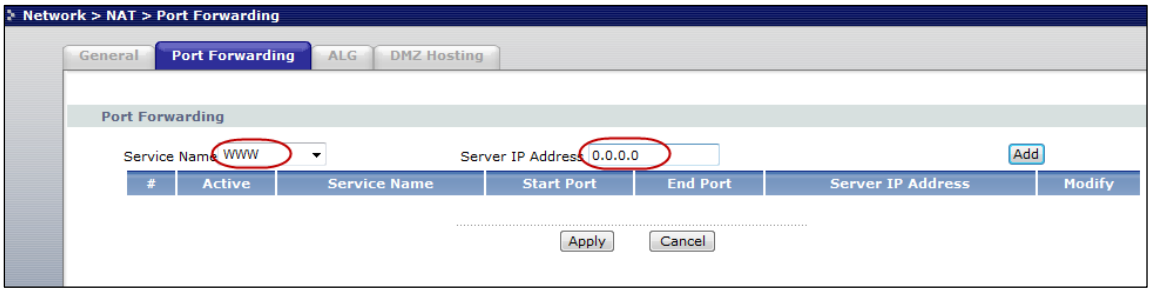
The following procedures show how to configure a server behind NAT.

Step 1: Login Web Configurator, **Network -> NAT -> Port Forwarding**

Step 2: Select the service name from the pull-down menu, and fill in the server

All contents copyright © 2011 ZyXEL Communications Corporation.

Address on '**Server IP Address**', then click button '**Add**' to save it.



Step 3: You could click the button 'Edit' on the rule to modify the Service name, Server IP Address, Start/End Port.

The most often used port numbers are shown in the following table. Please refer RFC 1700 for further information about port numbers.

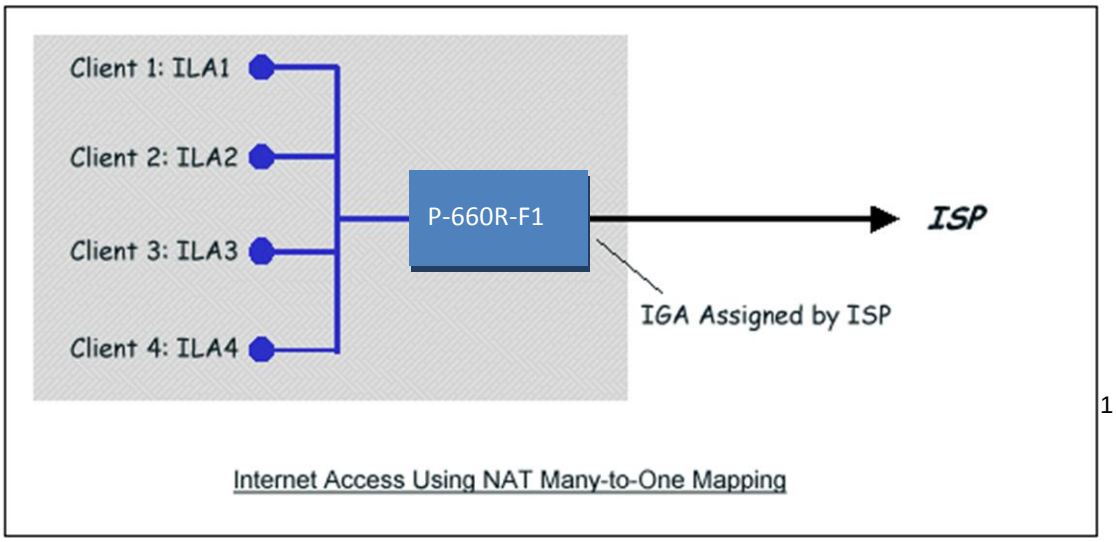
Service	Port Number
FTP	21
Telnet	23
SMTP	25
DNS (Domain Name Server)	53
www-http (Web)	80
PPTP (Point-to-Point Tunneling Protocol)	1723

Examples

Internet Access Only
Internet Access with an Internal Server
Using Multiple Global IP addresses for clients and servers
Support Non NAT Friendly Applications

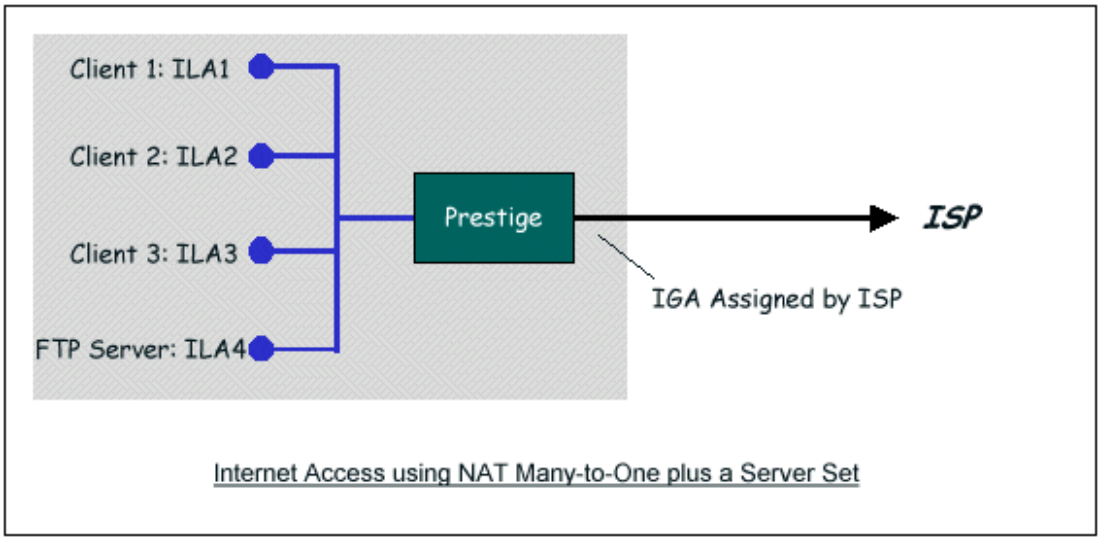
(1) Internet Access Only

In our Internet Access example, we only need one rule where all our ILAs map to one IGA assigned by the ISP. See the following figure.

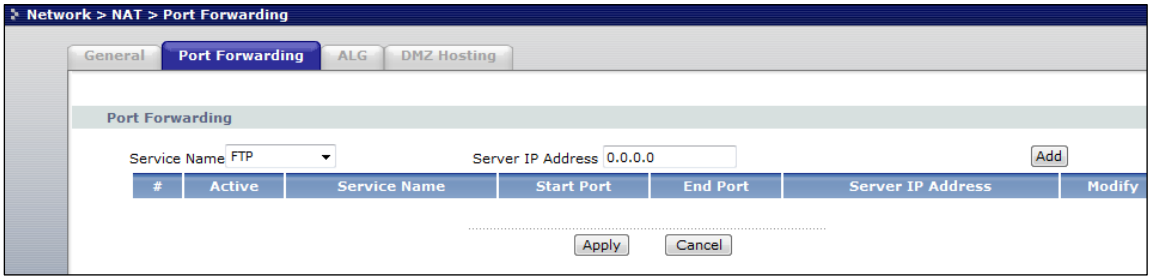


Internet Access Using NAT Many-to-One Mapping

(2) Internet Access with an Internal Server



In this case, we do exactly as the figure (use the convenient pre-configured SUA Only set) and also go to Web Configurator, Advanced Setup, **Network -> NAT -> Port Forwarding** to specify the Internet Server behind the NAT as below:



5. Using the Dynamic DNS (DDNS)

What is DDNS?

The DDNS service, an IP Registry provides a public central database where information such as email addresses, hostnames; IPs etc. can be stored and retrieved. This solves the problems if your DNS server uses an IP associated with dynamic IPs.

Without DDNS, we always tell the users to use the WAN IP of the P-660R-F1 to access the internal server. It is inconvenient for the users if this IP is dynamic. With DDNS supported by the P-660R-F1, you apply a DNS name (e.g., www.zyxel.com.tw) for your server (e.g., Web server) from a DDNS server. The outside users can always access the web server using the www.zyxel.com.tw regardless of the WAN IP of the P-660R-F1. When the ISP assigns the P-660R-F1 a new IP, the P-660R-F1 must inform the DDNS server the change of this IP so that the server can update its IP -to-DNS entry. Once the IP-to-DNS table in the

All contents copyright © 2011 ZyXEL Communications Corporation.

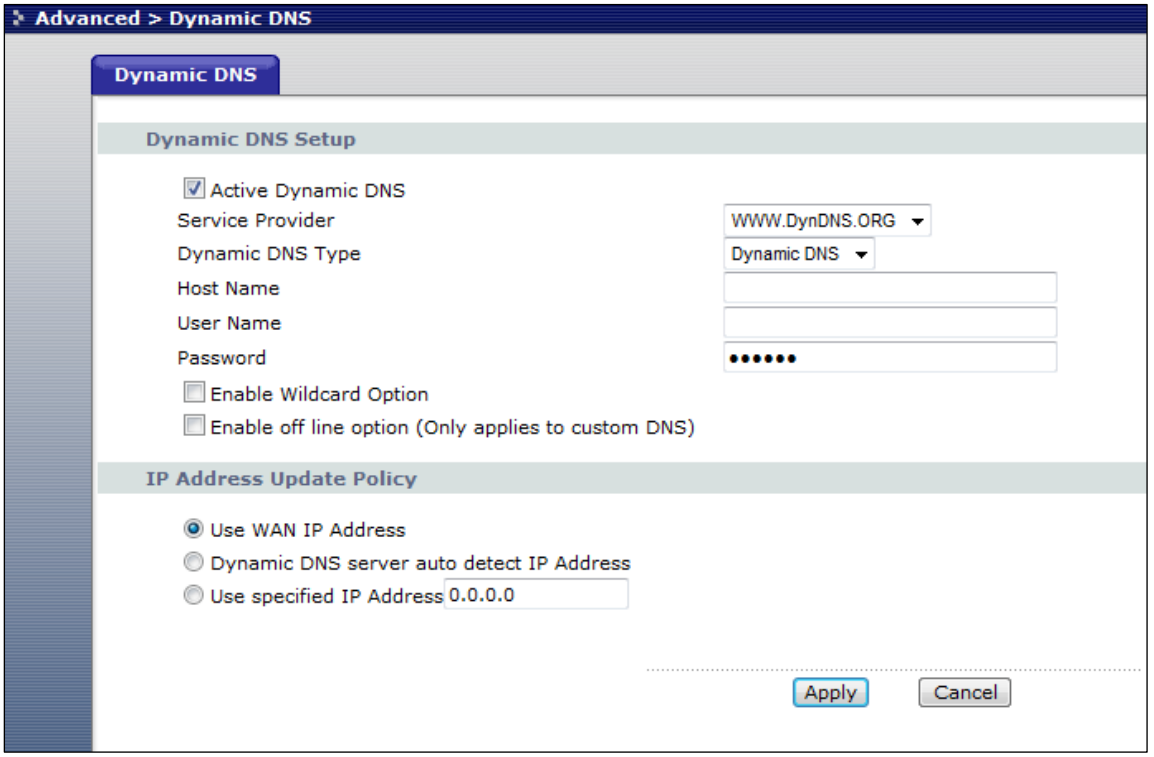
DDNS server is updated, the DNS name for your web server (i.e., www.zyxel.com.tw) is still usable.

The DDNS server the P-660R-F1 supports currently is WWW.DYNDNS.ORG where you apply the DNS from and update the WAN IP to.

Setup the DDNS

1. Before configuring the DDNS settings in the P-660R-F1, you must register an account from the DDNS server such as WWW.DYNDNS.ORG first. After the registration, you have a hostname for your internal server and a password using to update the IP to the DDNS server.

2. Login Web Configurator, Advanced Setup, **Advanced -> Dynamic DNS** Select **'Actived Dynamic DNS'** option:



Key Settings:

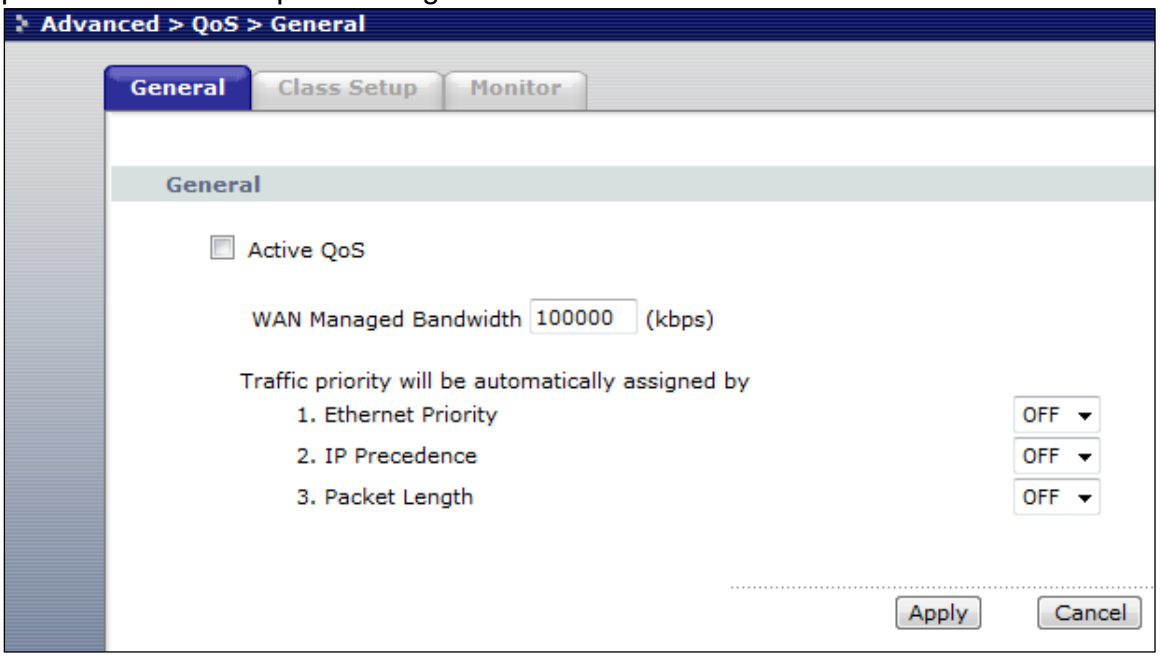
Option	Description
Service Provider	Currently, we support WWW.DYNDNS.ORG.
Host Name	Enter the hostname you subscribe from the above DDNS server. For example, zyxel.com.tw.
User Name	Enter the user name that the DDNS server gives to you.
Password	Enter the password that the DDNS server gives to you.

All contents copyright © 2011 ZyXEL Communications Corporation.

Enable Wildcard Option	Enter the hostname for the wildcard function that the WWW.DYNDNS.ORG supports. Note that Wildcard option is available only when the provider is http://www.dyndns.org/.

6. QoS (802.1Q)

The QoS General Screen
Click Advanced > QoS to open the screen as shown next.Use this screen to enable or disable QoS, and select to have the ZyXEL Device automatically assign priority to traffic according to the IEEE 802.1p priority level, IP precedence and/or packet length.



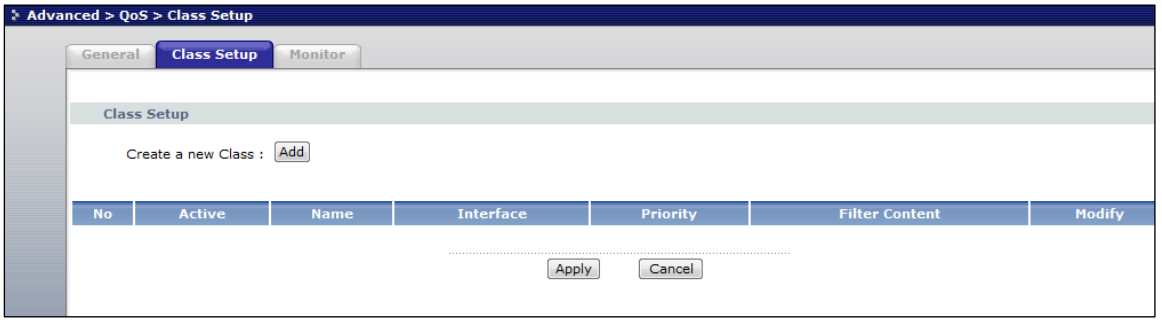
The following table describes the labels in this screen.

All contents copyright © 2011 ZyXEL Communications Corporation.

LABEL	DESCRIPTION
Active QoS	Select the check box to turn on QoS to improve your network performance. You can give priority to traffic that the ZyXEL Device forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.
WAN Managed Bandwidth	Enter the amount of bandwidth for the WAN interface that you want to allocate using QoS. The recommendation is to set this speed to match the interface's actual transmission speed. For example, set the WAN interface speed to 100000 kbps if your Internet connection has an upstream transmission speed of 100 Mbps. You can set this number higher than the interface's actual transmission speed. This will stop lower priority traffic from being sent if higher priority traffic uses all of the actual bandwidth. You can also set this number lower than the interface's actual transmission speed. This will cause the ZyXEL Device to not use some of the interface's available bandwidth.
Traffic priority will be automatically assigned by	These fields are ignored if traffic matches a class you configured in the **Class Setup** screen. If you select **ON** and traffic does not match a class configured in the **Class Setup** screen, the ZyXEL Device assigns priority to unmatched traffic based on the IEEE 802.1p priority level, IP precedence and/or packet length. If you select **OFF**, traffic which does not match a class is mapped to queue two.
Apply	Click **Apply** to save your settings back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

The Class Setup Screen

Use this screen to add, edit or delete classifiers. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming interface. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.



The following table describes the labels in this screen.

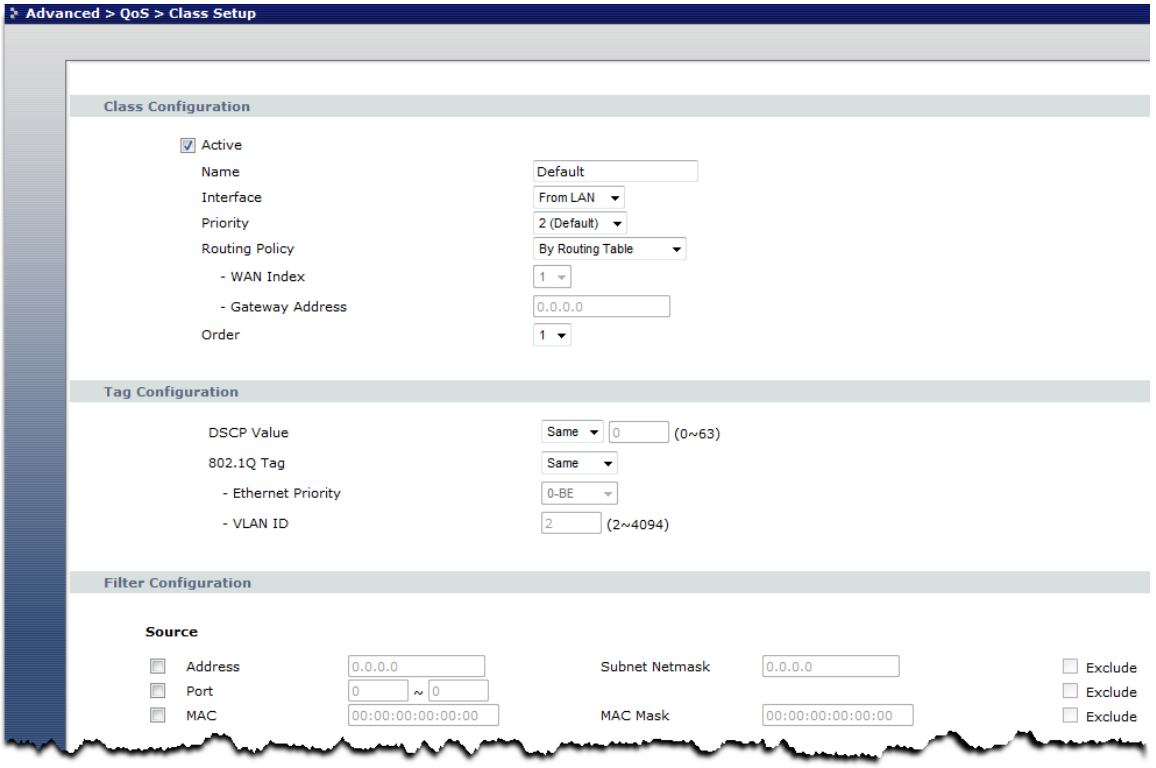
LABEL	DESCRIPTION
Create a new Class	Click **Add** to create a new classifier.
No	This is the number of each classifier. The ordering of the classifier is important as the classifiers are applied in turn.
Active	Select the check box to enable this classifier.
Name	This is the name of the classifier.

All contents copyright © 2011 ZyXEL Communications Corporation.

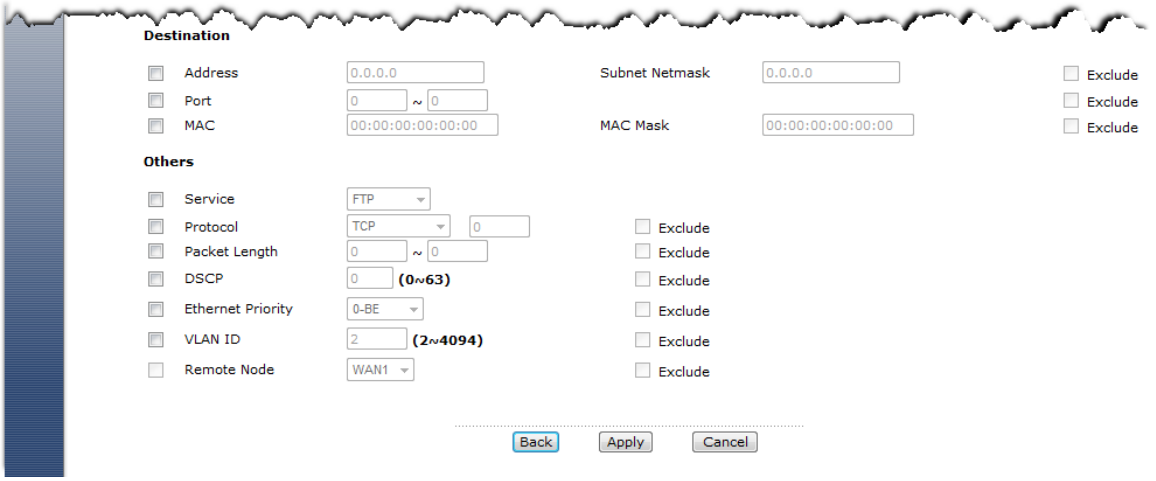
Interface	This shows the interface from which traffic of this classifier should come.
Priority	This is the priority assigned to traffic of this classifier.
Filer Content	This shows criteria specified in this classifier.
Modify	Click the Edit icon to go to the screen where you can edit the classifier. Click the Remove icon to delete an existing classifier.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

The Class Configuration Screen

Click the **Add** button or the **Edit** icon in the **Modify** field to configure a classifier.



All contents copyright © 2011 ZyXEL Communications Corporation.



The following table describes the labels in this screen.

LABEL	DESCRIPTION
Class Configuration	
Active	Select the check box to enable this classifier.
Name	Enter a descriptive name of up to 20 printable English keyboard characters, including spaces.
Interface	Select from which interface traffic of this class should come.
Priority	Select a priority level (between 0 and 7) or select **Auto** to have the ZyXEL Device map the matched traffic to a queue according to the internal QoS mapping table. "0" is the lowest priority level and "7" is the highest.
Routing Policy	Select the next hop to which traffic of this class should be forwarded. Select **By Routing Table** to have the ZyXEL Device use the routing table to find a next hop and forward the matched packets automatically. Select **To WAN Index** to route the matched packets through the specified PVC. This option is available only when the WAN type is ADSL. Select **Gateway Address** to route the matched packets to the router or switch you specified in the **Gateway Address** field.
WAN Index	Select a PVC index number.
Gateway Address	Enter the IP address of the gateway, which should be a router or switch on the same segment as the ZyXEL Device's interface(s), that can forward the packet to the destination.
Order	This shows the ordering number of this classifier. Select an existing number for where you want to put this classifier and click **Apply** to move the classifier to the number you selected. For example, if you select 2, the classifier you are moving becomes number 2 and the previous classifier 2 gets pushed down one.

All contents copyright © 2011 ZyXEL Communications Corporation.

Tag Configuration	
DSCP Value	Select **Same** to keep the DSCP fields in the packets. Select **Auto** to map the DSCP value to 802.1 priority level automatically. Select **Mark** to set the DSCP field with the value you configure in the field provided.
802.1Q Tag	Select **Same** to keep the priority setting and VLAN ID of the frames. Select **Auto** to map the 802.1 priority level to the DSCP value automatically. Select **Remove** to delete the priority queue tag and VLAN ID of the frames. Select **Mark** to replace the 802.1 priority field and VLAN ID with the value you set in the fields below. Select **Add** to treat all matched traffic untagged and add a second priority queue tag and VLAN.
Ethernet Priority	Select a priority level (between 0 and 7) from the drop down list box.
VLAN ID	Specify a VLAN ID number between 2 and 4094.
Filter Configuration	Use the following fields to configure the criteria for traffic classification.
Source	
Address	Select the check box and enter the source IP address in dotted decimal notation and the source subnet mask. A blank source IP address means any source IP address. Refer to the appendix for more information on IP subnetting.
Port	Select the check box and enter the port number of the source. 0 means any source port number.

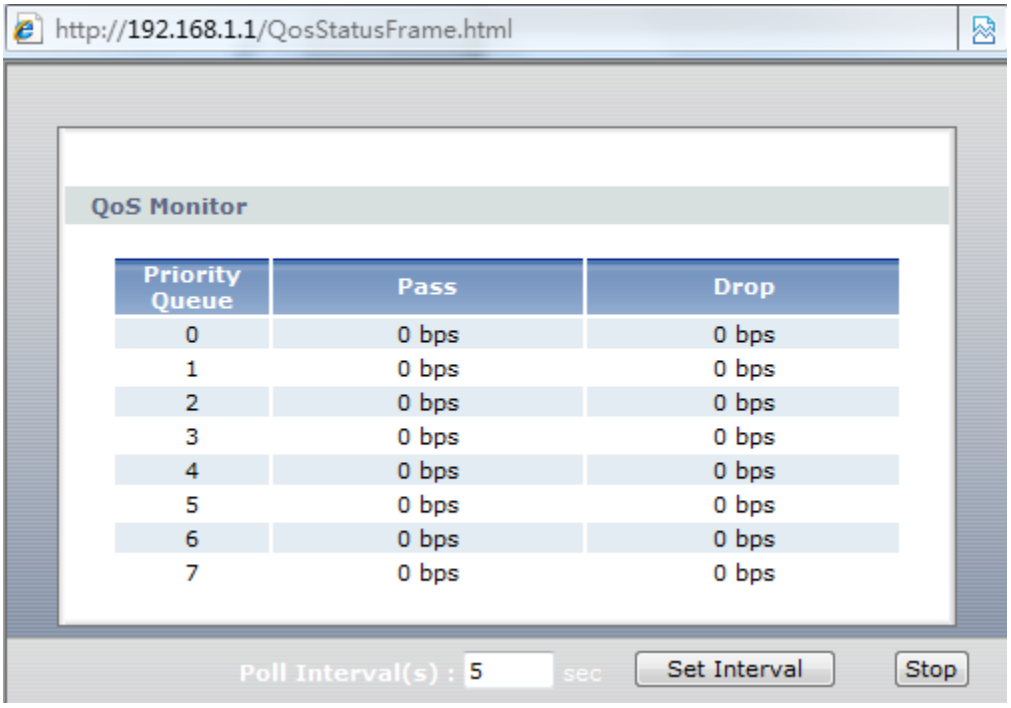
LABEL	DESCRIPTION
MAC	Select the check box and enter the source MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Destination	
Address	Select the check box and enter the destination IP address in dotted decimal notation and the destination subnet mask. Refer to the appendix for more information on IP subnetting.
Port	Select the check box and enter the port number of the destination. 0 means any source port number.
MAC	Select the check box and enter the destination MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified destination MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.

All contents copyright © 2011 ZyXEL Communications Corporation.

Others	
Service	This field simplifies classifier configuration by allowing you to select a predefined application. When you select a predefined application, you do not configure the rest of the filter fields. SIP (Session Initiation Protocol) is a signaling protocol used in Internet telephony, instant messaging and other VoIP (Voice over IP) applications. Select the check box and select **VoIP(SIP)** from the drop-down list box to configure this classifier for traffic that uses SIP. File Transfer Protocol (FTP) is an Internet file transfer service that operates on the Internet and over TCP/IP networks. A system running the FTP server accepts commands from a system running an FTP client. The service allows users to send commands to the server for uploading and downloading files. Select the check box and select **FTP** from the drop-down list box to configure this classifier for FTP traffic.
Protocol	Select this option and select the protocol (**TCP** or **UDP**) or select **User defined** and enter the protocol (service type) number. 0 means any protocol number.
Packet Length	Select this option and enter the minimum and maximum packet length (from 28 to 1500) in the fields provided.
DSCP	Select this option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
Ethernet Priority	Select this option and select a priority level (between 0 and 7) from the drop down list box. "0" is the lowest priority level and "7" is the highest.
VLAN ID	Select this option and specify a VLAN ID number between 2 and 4094.

The QoS Monitor Screen

To view the ZyXEL Device's QoS packet statistics, click **Advanced > QoS > Monitor**. The screen appears as shown.



The following table describes the labels in this screen.

All contents copyright © 2011 ZyXEL Communications Corporation.

LABEL	DESCRIPTION
Priority Queue	This shows the priority queue number. Traffic assigned to higher index queues gets through faster while traffic in lower index queues is dropped if the network is congested.
Pass	This shows how many packets mapped to this priority queue are transmitted successfully.
Drop	This shows how many packets mapped to this priority queue are dropped.
Poll Interval(s)	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the **Poll Interval(s)** field.
Stop	Click **Stop** to stop refreshing statistics.

7. Network Management Using SNMP

ZyXEL SNMP Implementation

ZyXEL currently includes SNMP support in some P-660R-F1 routers. It is implemented based on the SNMPv1, so it will be able to communicate with SNMPv1 NMSs. Further, users can also add ZyXEL's private MIB in the NMS to monitor and control additional system variables. The ZyXEL's private MIB tree is shown in figure 3. For SNMPv1 operation, ZyXEL permits one community string so that the router can belong to only one community and allows trap messages to be sent to only one NMS manager.

Some traps are sent to the SNMP manager when anyone of the following events happens:

1. coldStart (defined in RFC-1215) :

If the machine coldstarts, the trap will be sent after booting.

2. warmStart (defined in RFC-1215) :

If the machine warmstarts, the trap will be sent after booting.

3. linkDown (defined in RFC-1215) :

If any link of IDSL or WAN is down, the trap will be sent with the port number . The port number is its interface index under the interface group.

4. linkUp (defined in RFC-1215) :

If any link of IDSL or WAN is up, the trap will be sent with the port number . The port number is its interface index under the interface group.

5. authenticationFailure (defined in RFC -1215) :

When receiving any SNMP get or set requirement with wrong community, this trap is sent to the manager.

All contents copyright © 2011 ZyXEL Communications Corporation.

6. whyReboot (defined in ZYXEL-MIB) :

When the system is going to restart (warmstart), the trap will be sent with the reason of restart before rebooting.

(1) For intentional reboot:
In some cases (download new files, CI command "sys reboot", ...), reboot is done intentionally. And traps with the message "System reboot by user !" will be sent.

(2) For fatal error:
System has to reboot for some fatal errors. And traps with the message of the fatal code will be sent.

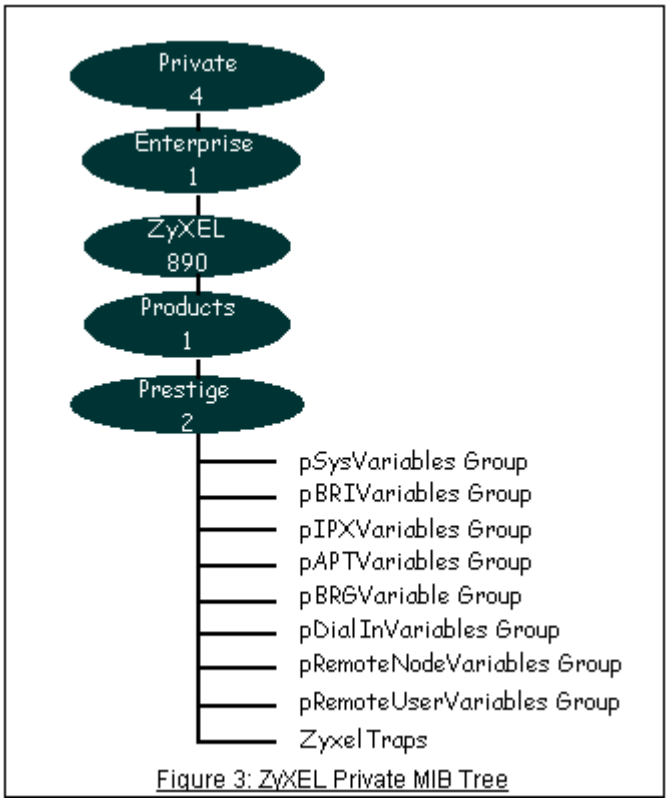
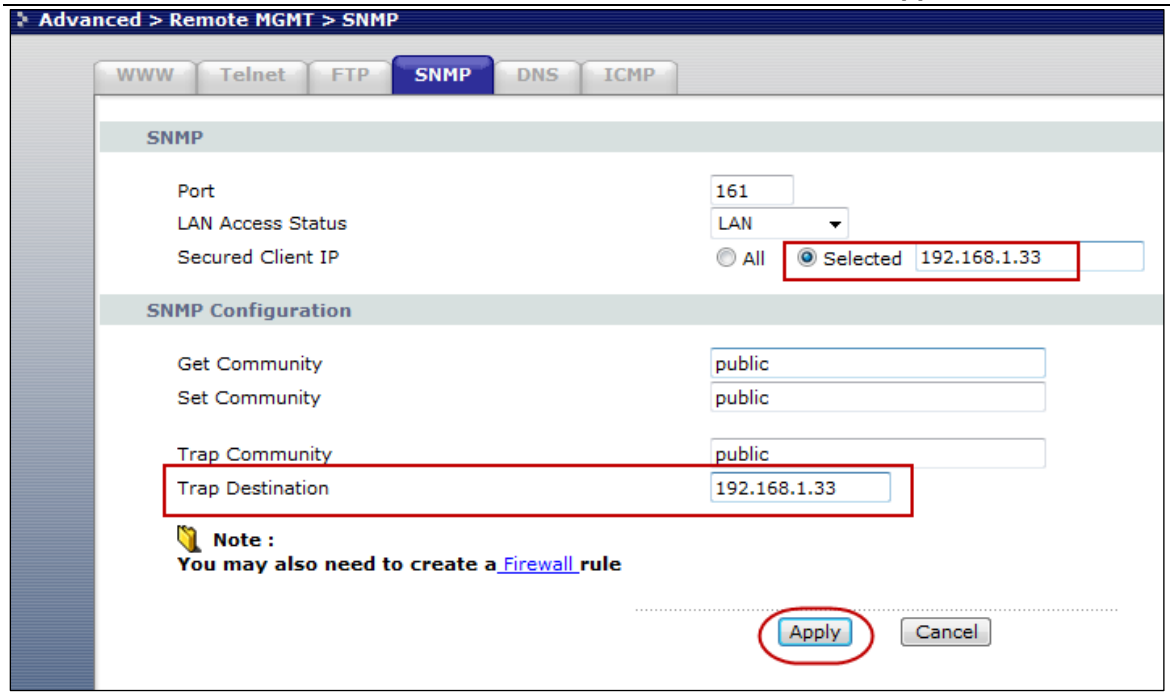


Figure 3: ZyXEL Private MIB Tree

The SNMP related settings in P-660R-F1 are configured in Web Configurator, Advanced Setup, **Advanced -> Remote MGNT -> SNMP** The following steps describe a simple setup procedure for configuring all SNMP settings.

All contents copyright © 2011 ZyXEL Communications Corporation.

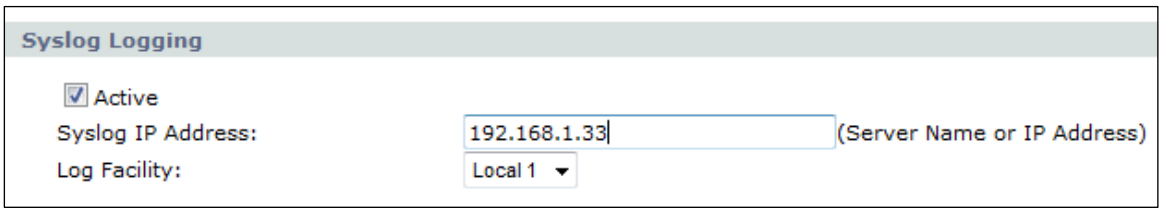


Key Settings:

Option	Descriptions
Get Community	Enter the correct Get Community. This Get Community must match the 'Get-' and 'GetNext' community requested from the NMS. The default is 'public'.
Set Community	Enter the correct Set Community. This Set Community must match the 'Set-community requested from the NMS. The default is 'public'.
Trusted Host	Enter the IP address of the NMS. The P-660R-F1HW-DX will only respond to SNMP messages coming from this IP address. **If 0.0.0.0 is entered, the P-660R-F1HW-DX will respond to all NMS managers.**
Trap Community	Enter the community name in each sent trap to the NMS. This Trap Community must match what the NMS is expecting. The default is 'public'.
Trap Destination	Enter the IP address of the NMS that you wish to send the traps to. **If 0.0.0.0 is entered, the P-660R-F1HW-DX will not send trap any NMS manager.**

Note: You may need to edit a firewall rule to permit SNMP Packets.

8. Using syslog



You can configure it in Web Configurator, Advanced Setup, **Maintenance -> Logs -> Log Settings -> Syslog logging.**

All contents copyright © 2011 ZyXEL Communications Corporation.

Key Settings:

Active: Select it to active UNIX Syslog.

Syslog IP Address: Enter the IP address of the UNIX server that you wish to send the syslog.

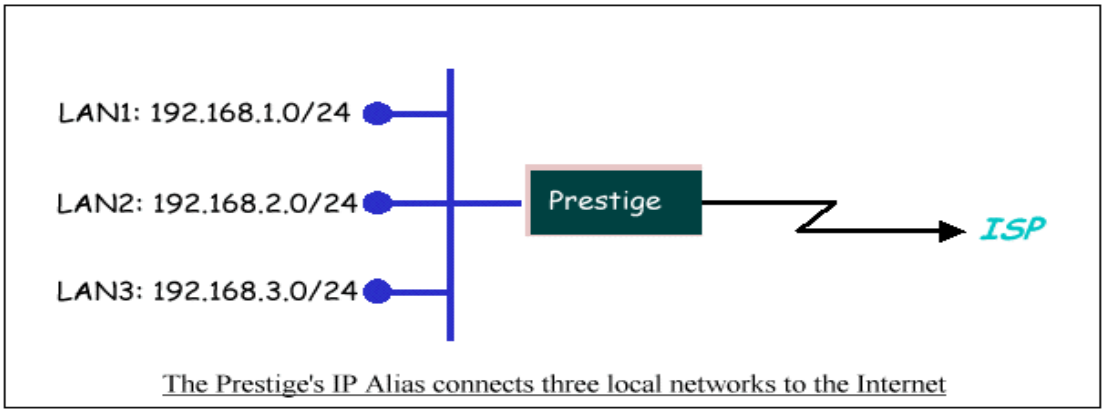
Log Facility: Select from the 7 different local options. The log facility lets you log the message in different server files. Refer to your UNIX manual.

All contents copyright © 2011 ZyXEL Communications Corporation.

9. Using IP Alias

What is IP Alias?

In a typical environment, a LAN router is required to connect two local networks. The P-660R-F1 can connect three local networks to the ISP or a remote node; we call this function as **'IP Alias'**. In this case, an internal router is not required. For example, the network manager can divide the local network into three networks and connect them to the Internet using P-660R-F1's single user account. See the figure below.

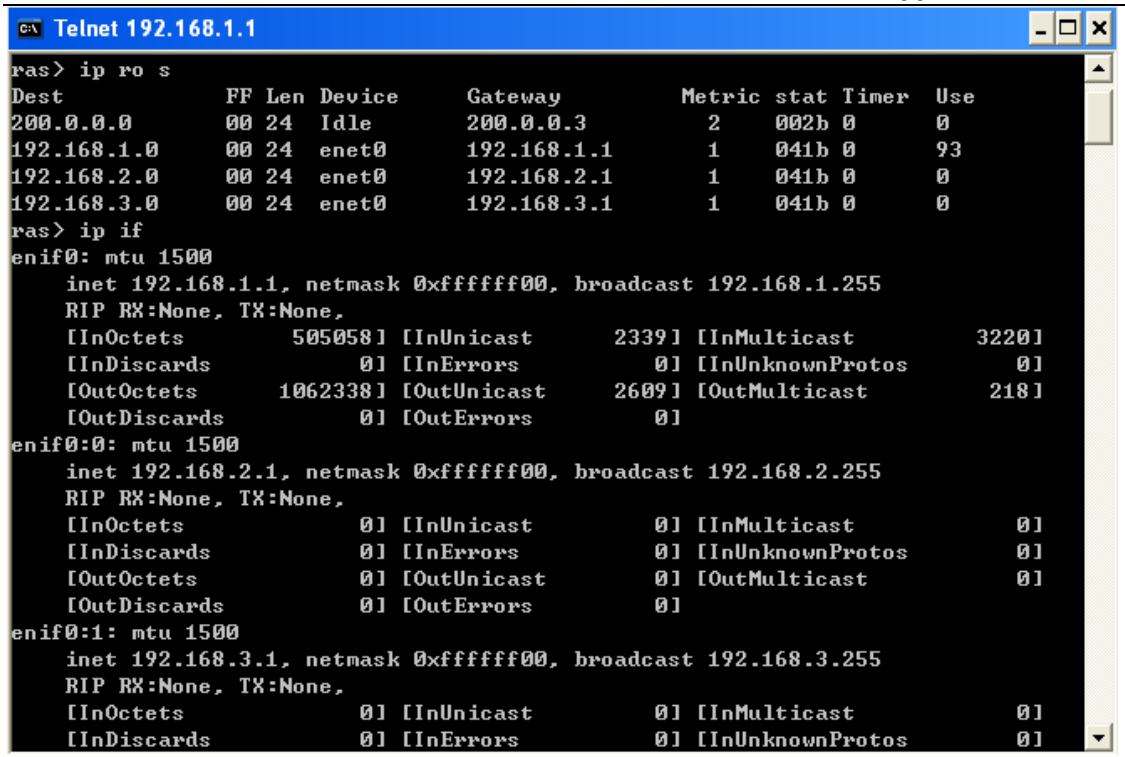


The Prestige's IP Alias connects three local networks to the Internet

The P-660R-F1 supports three virtual LAN interfaces via its single physical Ethernet interface. The first network can be configured in Web Configurator, Advanced Setup, **Network -> LAN -> DHCP Setup**. The second and third networks that we call **'IP Alias 1'** and **'IP Alias 2'** can be configured in **Network -> LAN -> IP Alias**.

There are three internal virtual LAN interfaces for the P-660R-F1 to route the packets from/to the three networks correctly. They are **enif0** for the major network, **enif0:0** for the IP alias 1 and **enif0:1** for the IP alias 2. Therefore, three routes are created in the P-660R-F1 as shown below when the three networks are configured. If the P-660R-F1's DHCP is also enabled, the IP pool for the clients can be any of the three networks.

All contents copyright © 2011 ZyXEL Communications Corporation.


Telnet 192.168.1.1
ras> ip ro s
Dest FF Len Device Gateway Metric stat Timer Use
200.0.0.0 00 24 Idle 200.0.0.3 2 002b 0 0
192.168.1.0 00 24 enet0 192.168.1.1 1 041b 0 93
192.168.2.0 00 24 enet0 192.168.2.1 1 041b 0 0
192.168.3.0 00 24 enet0 192.168.3.1 1 041b 0 0
ras> ip if
enif0: mtu 1500
inet 192.168.1.1, netmask 0xffffff00, broadcast 192.168.1.255
RIP RX:None, TX:None,
[InOctets 505058] [InUnicast 2339] [InMulticast 3220]
[InDiscards 0] [InErrors 0] [InUnknownProtos 0]
[OutOctets 1062338] [OutUnicast 2609] [OutMulticast 218]
[OutDiscards 0] [OutErrors 0]
enif0:0: mtu 1500
inet 192.168.2.1, netmask 0xffffff00, broadcast 192.168.2.255
RIP RX:None, TX:None,
[InOctets 0] [InUnicast 0] [InMulticast 0]
[InDiscards 0] [InErrors 0] [InUnknownProtos 0]
[OutOctets 0] [OutUnicast 0] [OutMulticast 0]
[OutDiscards 0] [OutErrors 0]
enif0:1: mtu 1500
inet 192.168.3.1, netmask 0xffffff00, broadcast 192.168.3.255
RIP RX:None, TX:None,
[InOctets 0] [InUnicast 0] [InMulticast 0]
[InDiscards 0] [InErrors 0] [InUnknownProtos 0]

You can edit filter rule to accept or deny LAN packets from/to the IP alias 1/2 go through the P-660R-F1 by command in **CLI**:

lan index [index number]
Usage: index number =1 main LAN
2 IP Alias#1
3 IP Alias#2

lan filter <incoming|outgoing> <tcpip|generic> [set#]
Usage: set#= the corresponding filter set number you've configured

lan save

- IP Alias Setup
-

(1) Edit the first network in Web Configurator, Advanced Setup, **Network -> LAN -> IP/DHCP Setup** by configuring the P-660R-F1's first LAN IP address.
Key Settings:

DHCP Setup	If the P-660R-F1's DHCP server is enabled, the IP pool for the clients can be any of the three networks.
TCP/IP Setup	Enter the first LAN IP address for the P-660R-F1. This will create the first route in the enif0 interface.

(2) Edit the second and third networks in **Network -> LAN -> IP Alias** by configuring the P-660R-F1's second and third LAN IP addresses.
Key Settings:

IP Alias 1	Active it and enter the second LAN IP address for the P-660R-F1.

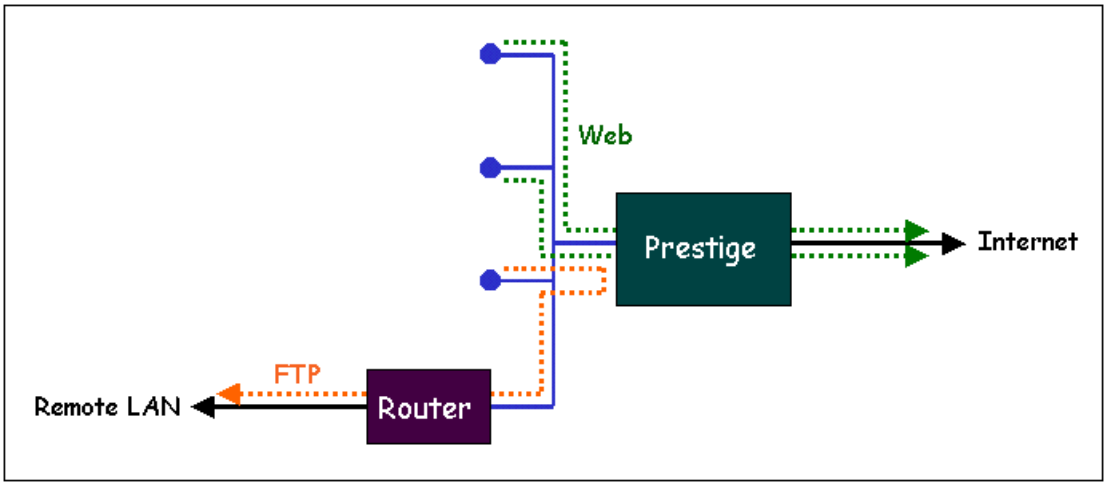
All contents copyright © 2011 ZyXEL Communications Corporation.

	This will create the second route in the enif0:0 interface.
IP Alias 2	Active it and enter the third LAN IP address for the P-660R-F1. This will create the third route in the enif0:1 interface.

10. Using IP Policy Routing

- What is IP Policy Routing (IPPR)?
-

Traditionally, routing is based on the destination address only and the router takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator.
Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing. Network administrators can use IPPR to distribute traffic among multiple paths. For example, if a network has both the Internet and remote node connections, we can route the Web packets to the Internet using one policy and route the FTP packets to the remote LAN using another policy. See the figure below.



Use IPPR to distribute traffic among multiple paths

- Benefits
-

Source-Based Routing - Network administrators can use policy-based routing to direct traffic from different users through different connections.
Quality of Service (QoS)- Organizations can differentiate traffic by setting the precedence or TOS (Type of Service) values in the IP header at the periphery of the network to enable the backbone to prioritize traffic.
Cost Savings- IPPR allows organizations to distribute interactive traffic on high-bandwidth, high-cost path while using low-path for batch traffic.
Load Sharing- Network administrators can use IPPR to distribute traffic among multiple paths.

- How does the IPPR work?
-

A policy defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. The criteria include the source address and port, IP protocol (ICMP, UDP, TCP,etc),

All contents copyright © 2011 ZyXEL Communications Corporation.

destination address and port, TOS and precedence (fields in the IP header) and length. The inclusion of length criterion is to differentiate between interactive and bulk traffic. Interactive applications, e.g., Telnet, tend to have short packets, while bulk traffic, e.g., file transfer, tends to have large packets.

The actions that can be taken include routing the packet to a different gateway (and hence the outgoing interface) and the TOS and precedence fields in the IP header. IPPR follows the existing packet filtering facility of ZyNOS in style and in implementation. The policies are divided into sets, where related policies are grouped together. A use defines the policies before applying them to an interface or a remote node, in the same fashion as the filters. There are 12 policy sets with 6 policies in each set.

- Setup the IP Policy Routing
-

Setp 1: Set the index of IP routing policy set rule by command '**ip policyrouting set index [set#] [rule#]**'. Suppose set#=1, rule#=1 in this example.

Step 2: Suppose we'd like to edit the rule like this:

```
Policy Set Name=Test
Active= Yes
Criteria:
IP Protocol     = 6
Type of Service= Don't Care        Packet length= 0
Precedence      = Don't Care         Len Comp= N/A
Source:
  addr start= 192.168.1.2          end= 192.168.1.20
  port start= 0                  end= N/A
Destination:
  addr start= 0.0.0.0              end= N/A
  port start= 80                 end= 80
Action= Matched
Gateway addr    = 192.168.1.254      Log= No
Type of Service= No Change
Precedence      = No Change
```

This policy example forces the Web packets originated from the clients with IP addresses from 192.168.1.2 to 192.168.1.20 be routed to the remote LAN via the gateway 192.168.1.254.
To implement this, we need to invoke the following command one by one:
ip policyrouting set name Test
(Set the name as Test of IP routing policy rule)
ip policyrouting set active yes
(Enable the rule)
ip policyrouting set criteria protocol 6
(Set the protocol ID as 6(TCP) for the rule)
ip policyrouting set criteria serviceType 0
(Set the criteria type of service as don't care for this rule)
ip policyrouting set criteria precedence 8
(Set the precedence as don't care for this rule)
ip policyrouting set criteria packetlength 0
(Set the packet length as 0 for the rule)
ip policyrouting set criteria srcip 192.168.1.2 192.168.1.20

All contents copyright © 2011 ZyXEL Communications Corporation.

(Set the source IP address for the rule: Start=192.168.1.2, end=192.168.1.20)
ip policyrouting set criteria srcport 0
(Set the source port for the rule: Start=0)
ip policyrouting set criteria destip 0.0.0.0
(Set the destination port for the rule: Start=0.0.0.0)
ip policyrouting set criteria destport 80 80
(Set the destination port for the rule: Start=80, end=80)
ip policyrouting set action actmatched
(Set the action for the rule: Matched)
ip policyrouting set action gatewaytype 0
(Set gateway type for the rule: Gateway Address)
ip policyrouting set action gatewayaddr 192.168.1.254
(Set the gateway address for the rule: 192.168.1.254)
ip policyrouting set criteria serviceType 0
(Set the action type of service as don't care for this rule)
ip policyrouting set criteria precedence 8
(Set the action precedence as don't care for this rule)
ip policyrouting set action log no
(Set log option for the rule: no log)
ip polictrouting set save
(Save the rule)

Step 3: Apply the IP policy routing. There are two interfaces to apply the policy set, they are the LAN interface and WAN interface. It depends where the gateway specified in the policy rule is located. If the gateway you specified is located on the local LAN you apply the policy set in LAN interface. If the gateway you specified is located on the remote WAN site you apply the policy set in WAN interface.
Apply to WAN Interface (Suppose we apply it to remote node 1 in the example):
wan node index 1
wan node ippolicy 1

11. Using Call Scheduling

- What is Call Scheduling?
  Call scheduling enables the mechanism for the P-660R-F1 to run the remote node connection according to the pre-defined schedule. This feature is just like the scheduler ina video recorder which records the program according to the specified time. Users can apply at most 4 schedule sets in Remote Node. The remote node configured with the schedule set could be "Forced On", "Forced Down", "Enable Dial-On-Demand", or "Disable Dial-On-Demand" on specified date and time.

- How to configure a Call Scheduling?
  You can configure a call scheduling in CLI
  Suppose we want to edit a call schedule set like this:
  Call Schedule Set #=1
  Set name=Test
  Active= Yes
  Start Date(yyyy-mm-dd)= 2005 - 12 - 27
  How Often= Once
  Once:

All contents copyright © 2011 ZyXEL Communications Corporation.

Date(yyyy-mm-dd)= 2005 -12 -27
Start Time(hh:mm)= 12 : 00
Duration(hh:mm)= 16 : 00
Action= Enable Dial-on-demand

This schedule example permits a demand call on the line on 12:00 a.m., 2005-12-27. The maximum length of time this connection is allowed is 16 hours.

To implement this, we need to invoke the following command one by one:
wan callsch index 1
(Set call schedule index #= 1. You must apply this command first before you begin to configure call schedule)
wan callsch name Test
(Set the schedule name as Test)
wan callsch active Yes
(Enable schedule)
wan callsch startdate 2005 12 27
(Set schedule start date as 2005-12-27)
wan callsch oncedate 2005 12 27
(Set the schedule used just once, it works on 2005-12-27)
wan callsch starttime 12 00
(Set the schedule start time as 12:00)
wan callsch duration 16 00
(Set schedule duration time as 16 hours)
wan callsch action 2
(Set action as dial-on-demand)
wan callsch save
(Save the current call schedule set)

Key Settings:

Start Date	Start date of this schedule rule. It can be unmatched with weekday setting. For example, if Start Date is 2000/10/02(Monday), but Monday setting in weekday can be No.
Forced On	The node will always keep up during the setting period. It is equivalent to diable the idel timeout.
Forced Down	The node will always keep doen during the setting period. The connected remote node will be dropped.
Enable Dial-On-Demand	The remote node accepts Dial-on-demand during this period.
Disable Dial-On-Demand	The remote node denies any demand dial during the period. For the existing connected nodes, it will be dropped after idle timeout and no triggered up.
Start Time/ Duration	Start Time and Duration of this schedule.

- Apply the schedule to the Remote node
  Multiple scheduling rules can program in a Remote node, and they have priority. For example, if we program the sets as 1,2,3,4 in remote node, then the set 1 will override set 2,3,4. set 2 will override 3,4, and so on.

All contents copyright © 2011 ZyXEL Communications Corporation.

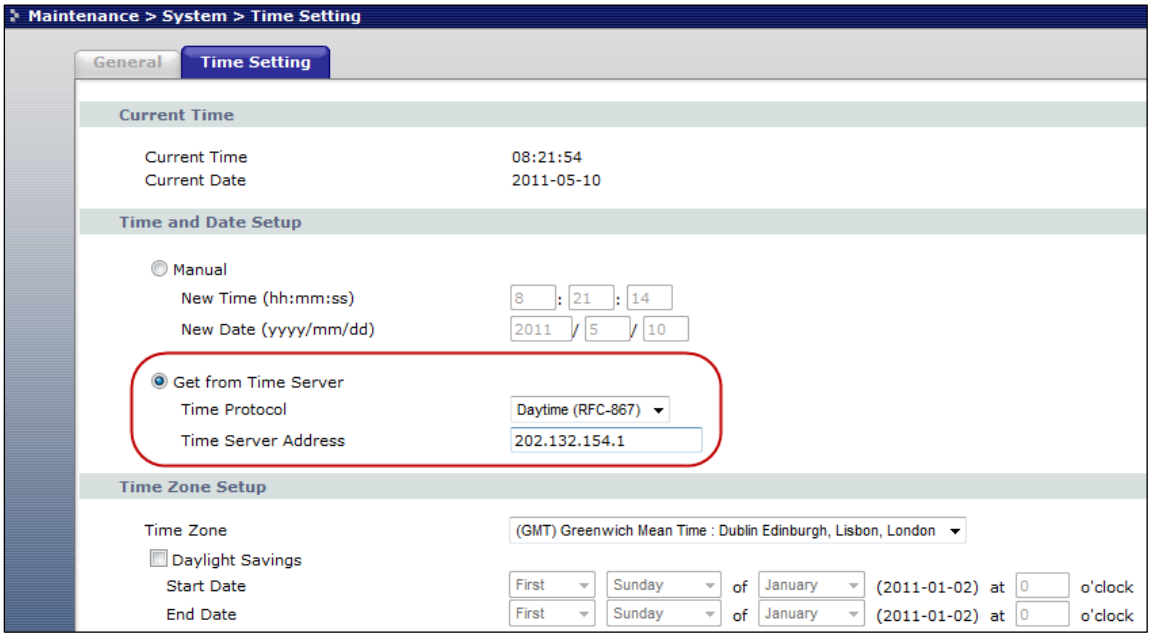
We can apply the schedule to the remote node in **CLI** by the commands:

wan node index []index#]
wan node callsch [index#]
wan node save

For example, if we want to apply the call schedule set 1 to remote node 1, we could use the commands:

wan node index 1
wan node callsch 1
wan node save

- Time Service in P-660R-F1
  There is no RTC (Real-Time Clock) chip so the P-660R-F1 should launch a mechanism to get current time and date from external server in boot time. Time service is implemented by the **Daytime protocol(RFC-867)**, **Time protocol(RFC-868)**, and **NTP protocol(RFC-1305)**. You have to assign an IP address of a time server and then, the P-660R-F1 will get the date, time, and time-zone information from this server. You can configure it in Web Configurator, Advanced Setup, **Maintenance -> System -> Time Setting.**



12. Using IP Multicast

What is IP Multicast?

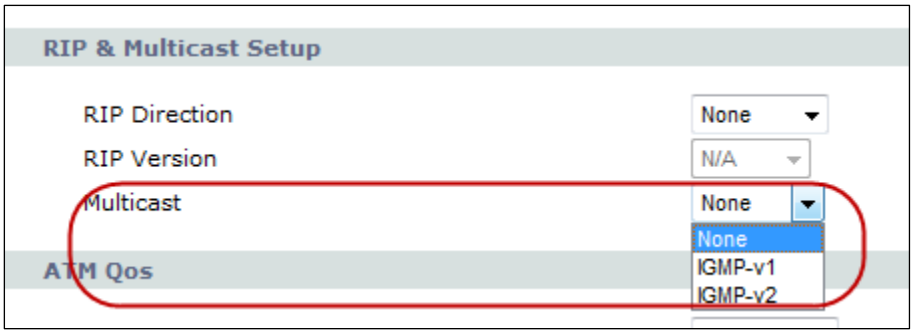
Traditionally, IP packets are transmitted in two ways - unicast or broadcast. Multicast is a third way to deliver IP packets to a group of hosts. Host groups are identified by class D IP addresses, i.e., those with "1110" as their higher-order bits. In dotted decimal notation, host group addresses range from 224.0.0.0 to 239.255.255.255. Among them, 224.0.0.1 is assigned to the permanent IP hosts group, and 224.0.0.2 is assigned to the multicast routers group.
IGMP (Internet Group Management Protocol) is the protocol used to support

All contents copyright © 2011 ZyXEL Communications Corporation.

multicast groups. The latest version is version 2 (see RFC2236). IP hosts use IGMP to report their multicast group membership to any immediate-neighbor multicast routers so the multicast routers can decide if a multicast packet needs to be forwarded. At start up, the P-660R-F1 queries all directly connected networks to gather group membership.
After that, the P-660R-F1 updates the information by periodic queries. The P-660R-F1 implementation of IGMP is also compatible with version 1. The multicast setting can be turned on or off on Ethernet and remote nodes.
P-660R-F1 supports IGMP v1 and v2 without source filtering.

- **IP Multicast Setup**
  (1) Enable IGMP in P-660R-F1's LAN in Web Configurator, Advanced Setup, **Network -> LAN -> IP -> Advanced Setup.**

  (2) Enable IGMP in P-660R-F1's remote node in Web Configurator, Advanced Setup, **Network -> WAN ->Internet Connection -> Advanced Setup.**



Key Settings:

Multicast	IGMP-v1 for IGMP version 1, IGMP-v2 for IGMP version 2.

13. Using Zero-Configuration

- **Zero-Configuration and VC auto-hunting**
  Zero-Configure feature can help customer to reduce the burden of setting efforts. Whenever system ADSL links up system will send out some probing patterns, system will analyze the packets returned from ISP, and decide which services the ISP may provide. Because ADSL is based on a ATM network, so system have to **pre-configured a VPI/VCI hunting pool before Auto-Configure function begins to** work.
  The Zero-Configuration feature can hunt the encapsulation and VPI/VCI value, and system will automatically configure itself if the hunting result is successfully. This feature has two constraints:
  1. It supports the ISP provides one kind of service (PPPoE/PPPoA, etc.) only, otherwise the hunting will get confusing and failed.
  2. VC auto-hunting only supports dynamic WAN IP address. If the router is set a static WAN IP address. VC auto-hunting function will be disabled.
  The entry of hunting pool must also contain the VPI, VCI, and which kinds of hunting patterns you wish to send. Whenever system send out all the probing patterns with specific VPI/VCI, system will wait for 5~10 seconds and get the response from ISP, the response patterns will decide which kinds of ADSL services of the line will be. After that, system will save back the correct VPI, VCI and also services (encapsulation) type into profile of WAN interface.

All contents copyright © 2011 ZyXEL Communications Corporation.

- **Configure the VC auto-hunting preconfigured table.**
  (1) Display auto-haunting preconfigured table by using command from **CLI**:
  wan atm vchunt disp

```
ras> wan atm vchunt disp
(1) Configure Buffer
(2) RemoteNode (Read Only)
 RN VPI   VCI  | RN VPI   VCI  | RN VPI   VCI  | RN VPI   VCI  |
-------------------------------------------------------------
  1   0    33 |  2   N     N |  3   N     N |  4   N     N |
  5   N     N |  6   N     N |  7   N     N |  8   N     N |
(3) VC Hunt Table: (User setting)
 Flags: Inactive(0)
 RN VPI   VCI serv| RN VPI   VCI serv| RN VPI   VCI serv| RN VPI  VCI serv
-------------------------------------------------------------
  1   0  35   22H|  0   0   0    0H|  0   0   0    0H|  0   0   0    0H|
  0   0   0    0H|  0   0   0    0H|  0   0   0    0H|  0   0   0    0H|
  0   0   0    0H|  0   0   0    0H|
(4) WebRedirect: Disable
```

(2) Add items to the auto-haunting preconfigured table by using commands:
wan atm vchunt add <remoteNodeIndex> <vpi> <vci> <service bit(hex)>
wan atm vchunt save

Note: <remote node> : input the remote node index 1-8
<vpi> : vpi value
<vci> : vci value
<service>: it's a hex value, bit0:PPPoE/VC (1), bit1:PPPoE/LLC (2) , bit2:PPPoA/VC (4), bit3:PPPoA/LLC (8), bit4:Enet/VC (16), bit5 :Enet/LLC (32)

For example:

(1) If you need service PPPoE/LLC and Enet/LLC then the service bits will be 2+32 = 34 (decimal) = 22 (hex), you must input 22

(2) If you want to enable all service for VC hunting, the service bits will be 1+2+4+8+16+32=63(decimal)= 3f (hex), you must input 3f

Need to perform save after this by command '**wan atm vchunt save**'

```
ras> wan atm vchunt add 1 8 36 3f
ras> wan atm vchunt save
ras> wan atm vchunt display
(1) Configure Buffer
(2) RemoteNode (Read Only)
 RN VPI   VCI  | RN VPI   VCI  | RN VPI   VCI  | RN VPI   VCI  |
-------------------------------------------------------------
  1   0    33 |  2   N     N |  3   N     N |  4   N     N |
  5   N     N |  6   N     N |  7   N     N |  8   N     N |
(3) VC Hunt Table: (User setting)
 Flags: Inactive(0)
 RN VPI   VCI serv| RN VPI   VCI serv| RN VPI   VCI serv| RN VPI  VCI serv
-------------------------------------------------------------
  1   0  35   22H|  1   8  36   3fH|  0   0   0    0H|  0   0   0    0H|
  0   0   0    0H|  0   0   0    0H|  0   0   0    0H|  0   0   0    0H|
  0   0   0    0H|  0   0   0    0H|
```

(3) Delete items from the auto-haunting preconfigured table by useing command:
wan atm vchunt remove <remote node> <vpi> <vci>

All contents copyright © 2011 ZyXEL Communications Corporation.

```
ras> wan atm vchunt remove 1 8 36
ras> wan atm vchunt display
(1) Configure Buffer
(2) RemoteNode (Read Only)
 RN VPI   VCI  : RN VPI   VCI  : RN VPI   VCI  : RN VPI   VCI  :
-------------------------------------------------------------
  1   0    33 :  2   N     N :  3   N     N :  4   N     N :
  5   N     N :  6   N     N :  7   N     N :  8   N     N :
(3) VC Hunt Table: (User setting)
 Flags: Inactive(0)
 RN VPI   VCI serv: RN VPI   VCI serv: RN VPI   VCI serv: RN VPI  VCI serv
-------------------------------------------------------------
  1   0  35   22H:  0   0   0    0H:  0   0   0    0H:  0   0   0    0H:
  0   0   0    0H:  0   0   0    0H:  0   0   0    0H:  0   0   0    0H:
  0   0   0    0H:  0   0   0    0H:
```


All contents copyright © 2011 ZyXEL Communications Corporation.

Support Tool

1. Firmware/Configurations Uploading and Downloading using TFTP

- **Using TFTP client software**
- Upload/download ZyNOS via LAN
- Upload/download Prestige configurations via LAN

(1) Using TFTP to upload/download ZyNOS via LAN

Step 1: TELNET to your Prestige first before running the TFTP software

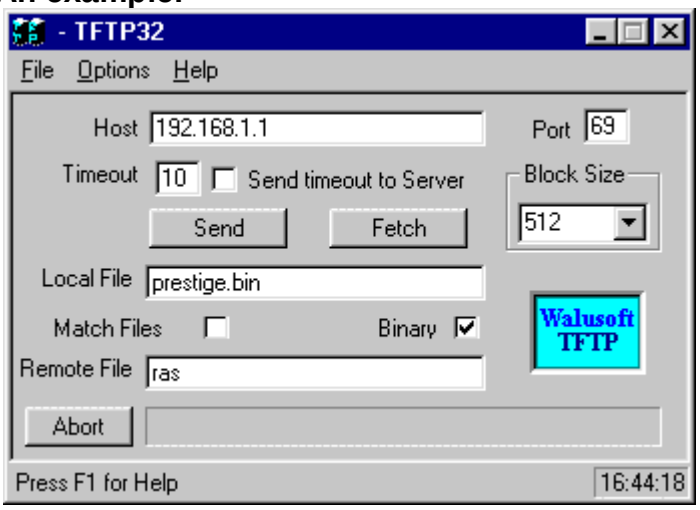
Step 2: Type the CI command **'sys stdio 0'** to disable console idle timeout in **Command Line Interface (CLI)**

Step 3: Run the TFTP client software

Step 4: Enter the IP address of the Prestige

Step 5:To upload the firmware, please save the remote file as **'ras'** to Prestige. After the transfer is complete, the Prestige will program the upgraded firmware into FLASH ROM and reboot itself.

An example:



The 192.168.1.1 is the IP address of the Prestige. The local file is the source file of the ZyNOS firmware that is available in your hard disk. The remote file is the file name that will be saved in Prestige. Check the port number 69 and 512-Octet blocks for TFTP. Check **'Binary'** mode for file transfering.

(2) Using TFTP to upload/download SMT configurations via LAN

Step 1: TELNET to your Prestige first before running the TFTP software

Step 2: Type the command **'sys stdio 0'** to disable console idle timeout in **Command Line Interface (CLI).**

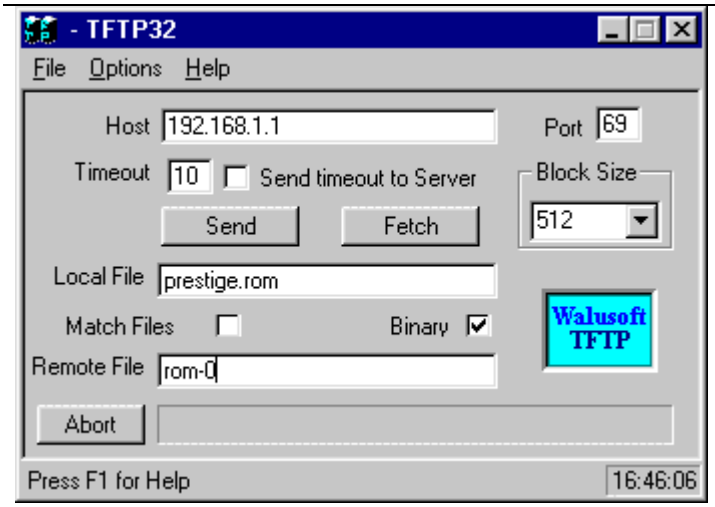
Step 3: Run the TFTP client software

Step 4: To download the P-660R-F1 configuration, please get the remote file **'rom-0'** from the Prestige.

Step 5: To upload the P-660R-F1 configuration, please save the remote file as **'rom-0'** in the Prestige.

An example:

All contents copyright © 2011 ZyXEL Communications Corporation.



- The 192.168.1.1 is the IP address of the Prestige.
- The local file is the source file of your configuration file that is available in your hard disk.
- The remote file is the file name that will be saved in Prestige.
- Check the port number 69 and 512-Octet blocks for TFTP.
- Check 'Binary' mode for file transfering.

- **Using TFTP command on Windows NT**
  Step 1: TELNET to your Prestige first before using TFTP command
  Step 2: Type the CI command **'sys stdio 0'** to disable console idle timeout in **Command Line Interface (CLI).**
  Step 3: Download ZyNOS via LAN : **c:\tftp -i [PrestigeIP] get ras [localfile]**
  Step 4: Upload P-660R-F1 configurations via LAN: **c:\tftp -i [PrestigeIP] put [localfile] rom-0**
  Step 5: Download P-660R-F1 configurations via LAN: **c:\tftp -i [PrestigeIP] get rom-0 [localfile]**
- **Using TFTP command on UNIX**
  Before you begin:

1. TELNET to your Prestige first before using TFTP command
2. Type the CI command 'sys stdio 0' to disable console idle timeout in **Command Line Interface (CLI)**
   Example:

```
[cppwu@faelinux cppwu]$ telnet 192.168.1.1
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
Password: ****
ras> sys stdio 0
(Open a new window)
[cppwu@faelinux cppwu]$ tftp -I 192.168.1.1 get rom-0 [local-rom] <- change to binary mode

<- download configurations
[cppwu@faelinux cppwu]$ tftp -I 192.168.1.1 put [local-rom] rom-0 <- upload configurations
[cppwu@faelinux cppwu]$ tftp -I 192.168.1.1 get ras [local-ras ] <- download firmware
[cppwu@faelinux cppwu]$ tftp -I 192.168.1.1 put [local-ras] ras <- upload
```


All contents copyright © 2011 ZyXEL Communications Corporation.

firmware

2. Using FTP to Upload the Firmware and Configuration Files

In addition to upload the firmware and configuration file via the console port and TFTP client, you can also upload the firmware and configuration files to the Prestige using FTP.

To use this feature, your workstation must have a FTP client software. See the example shown below.

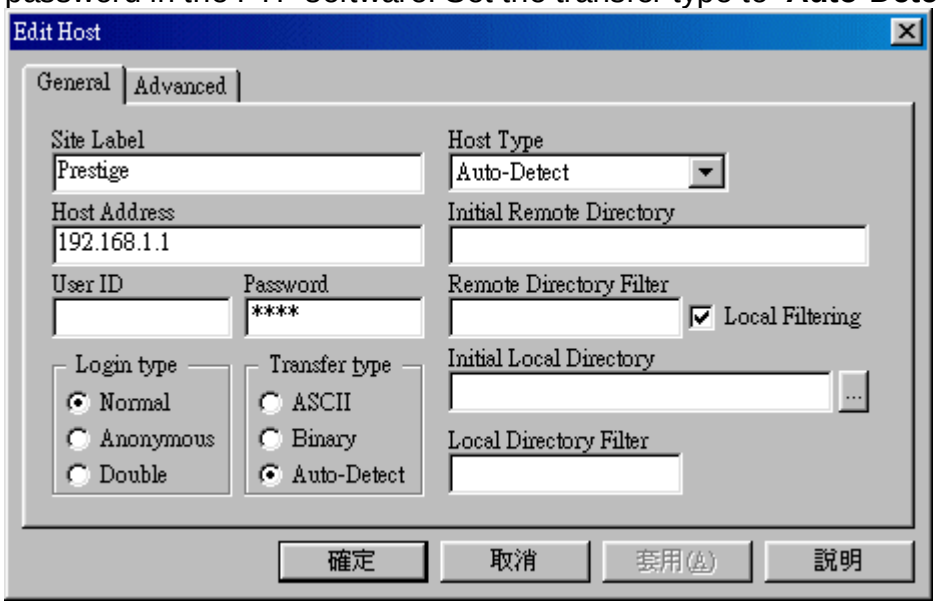
- **Using FTP client software**

  Note: The remote file name for the firmware is **'ras'** and the configuration file is **'rom-0'**.

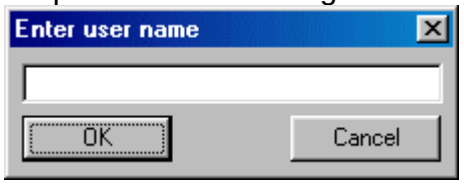
Step 1	Use FTP client from your workstation to connect to the Prestige by entering the IP address of the Prestige.
Step2	Press **'Enter'** key to ignore the username, because the Prestige does not check the username.
Step 3	Enter the **CLI** password as the FTP login password, the default is **'admin'**.
Step 4	Enter command **'bin'** to set the transfer type to binary.
Step 5	Use **'put'** command to transfer the file to the Prestige.

Example:

Step 1: Connect to the Prestige by entering the Prestige's IP and Administrator password in the FTP software. Set the transfer type to **'Auto-Detect'** or **'Binary'**.



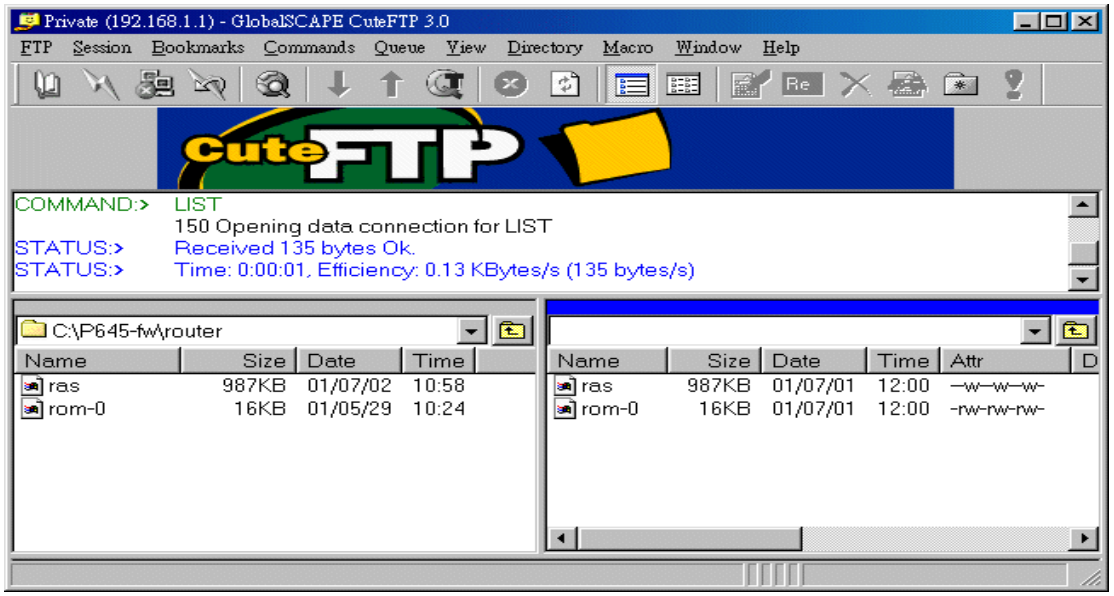
Step 2: Press **'OK'** to ignore the 'Username' prompt.



Step 3: To upload the firmware file, we transfer the local **'ras'** file to overwrite the remote **'ras'** file.

All contents copyright © 2011 ZyXEL Communications Corporation.

To upload the configuration file, we transfer the local **'rom-0'** to overwrite the remote **'rom-0'** file.


Private (192.168.1.1) - GlobalSCAPE CuteFTP 3.0
FTP Session Bookmarks Commands Queue View Directory Macro Window Help
CuteFTP
COMMAND:> LIST
150 Opening data connection for LIST
STATUS:> Received 135 bytes Ok.
STATUS:> Time: 0:00:01, Efficiency: 0.13 KBytes/s (135 bytes/s)
C:\P645-fw\router
Name Size Date Time
ras 987KB 01/07/02 10:58
rom-0 16KB 01/05/29 10:24
Name Size Date Time Attr
ras 987KB 01/07/01 12:00 -w--w--w-
rom-0 16KB 01/07/01 12:00 -rw-rw-rw-

Step 4: The Prestige reboots automatically after the uploading is finished. Please do not power off the router at this moment.

All contents copyright © 2011 ZyXEL Communications Corporation.

CI Command Reference

Command Syntax and General User Interface

CI has the following command syntax:

command <*iface* | *device* > **subcommand** [*param*]
command subcommand [*param*]
command ? **| help**
command subcommand ? | help

General user interface:

1.	**?**	Shows the following commands and all major (sub) commands
2.	**exit**	Exit Subcommand

To get the latest CI Command list

The latest CI Command list is available in release note of every ZyXEL firmware release. Please go to ZyXEL public WEB site http://www.zyxel.com/support/download_library/download_library_1_1.shtml to download firmware package (*.zip), you should unzip the package to get the release note in PDF format.

All contents copyright © 2011 ZyXEL Communications Corporation.